30 October 2015

The Honourable Annastacia Palaszczuk MP
Premier and Minister for the Arts
PO Box 15185
CITY EAST QLD 4002

Dear Premier,

In accordance with Commissions of Inquiry Order (No. 1) 2015, I have made full and careful inquiry into the extent, nature and impacts of organised crime in Queensland, and present the report of the Queensland Organised Crime Commission of Inquiry.

Yours sincerely,

Michael Byrne QC
Commissioner
Queensland Organised Crime Commission of Inquiry
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Executive summary</td>
<td>2</td>
</tr>
<tr>
<td>Recommendations</td>
<td>10</td>
</tr>
<tr>
<td>Chapter 1 Introduction</td>
<td>15</td>
</tr>
<tr>
<td>1.1 The Commission of Inquiry</td>
<td>16</td>
</tr>
<tr>
<td>1.2 The scope of the Inquiry</td>
<td>16</td>
</tr>
<tr>
<td>1.2.1 Exclusions</td>
<td>17</td>
</tr>
<tr>
<td>1.2.2 Defining ‘organised crime’</td>
<td>17</td>
</tr>
<tr>
<td>1.3 Process of the Inquiry</td>
<td>18</td>
</tr>
<tr>
<td>1.4 The 2013 legislation</td>
<td>20</td>
</tr>
<tr>
<td>Chapter 2 Outlaw Motorcycle Gangs</td>
<td>23</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>23</td>
</tr>
<tr>
<td>2.2 Outlaw motorcycle gang criminal activity</td>
<td>24</td>
</tr>
<tr>
<td>Chapter 3 The illicit drug market</td>
<td>27</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>27</td>
</tr>
<tr>
<td>3.2 High-threat illicit drugs</td>
<td>29</td>
</tr>
<tr>
<td>3.2.1 Methylamphetamine</td>
<td>29</td>
</tr>
<tr>
<td>3.2.2 Cocaine</td>
<td>64</td>
</tr>
<tr>
<td>3.2.3 Heroin</td>
<td>87</td>
</tr>
<tr>
<td>3.2.4 MDMA/’ecstasy’</td>
<td>103</td>
</tr>
<tr>
<td>3.2.5 Cannabis</td>
<td>123</td>
</tr>
<tr>
<td>3.2.6 Drug analogues and new psychoactive substances</td>
<td>146</td>
</tr>
<tr>
<td>3.3 The effect of illicit drug use on society</td>
<td>173</td>
</tr>
<tr>
<td>3.3.1 What effect does illicit drug use have on the community?</td>
<td>174</td>
</tr>
<tr>
<td>3.3.2 Conclusion</td>
<td>183</td>
</tr>
<tr>
<td>3.4 Legislation</td>
<td>188</td>
</tr>
<tr>
<td>3.4.1 Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987</td>
<td>188</td>
</tr>
<tr>
<td>3.4.2 Police powers in Queensland</td>
<td>204</td>
</tr>
<tr>
<td>3.4.3 Regulatory gaps</td>
<td>208</td>
</tr>
</tbody>
</table>
3.5 Related activities ............................................................................................................213
   3.5.1 The Internet 213
   3.5.2 Pharmacists 224
   3.5.3 Lawyers 234
   3.5.4 Violence and extortion 236
3.6 Responses to organised crime ..................................................................................246
   3.6.1 Queensland Police Service 246
   3.6.2 Crime and Corruption Commission 250
   3.6.3 Office of the Director of Public Prosecutions 252
3.7 Future trends in organised crime in the illicit drug market .......................................256

Chapter 4 Online child sexual offending & child exploitation material ..........................259
4.1 Introduction ...................................................................................................................259
4.2 Online child sexual offending ...................................................................................261
   4.2.1 Types of offending 261
   4.2.2 Prevalence of the offending 274
   4.2.3 Victim impacts and impacts on the community 282
4.3 Child exploitation material market ..........................................................................286
   4.3.1 Types of offending 286
   4.3.2 Prevalence of offending 293
   4.3.3 Victim impacts and impacts on the community 304
4.4 Related activities ............................................................................................................310
   4.4.1 Cyber and technology-enabled crime 310
   4.4.2 Violence and extortion 315
   4.4.3 IT experts and technical security experts 316
4.5 Legislation .......................................................................................................................318
   4.5.1 Legislative framework 318
   4.5.2 Legislative gaps or inadequacies 319
4.6 Responses to organised crime ...................................................................................357
   4.6.1 Queensland Police Service 357
   4.6.2 Crime and Corruption Commission 365
   4.6.3 Office of the Director of Public Prosecutions 367
4.7 Future trends and emerging markets ......................................................................369
6.3 How is money laundered? ................................................................. 504
  6.3.1 Banking 504
  6.3.2 Alternative remittance systems 506
  6.3.3 Casinos 508
  6.3.4 Bullion and jewellery 510
  6.3.5 Debit cards 511
  6.3.6 Digital currencies 512
  6.3.7 Real estate and real estate agents as facilitators 512
  6.3.8 Professional facilitators 515

6.4 Statutory review of Anti-Money Laundering and Counter Terrorism Financing Act ......................................................... 529

6.5 Conclusion ....................................................................................... 529

Chapter 7 Corruption......................................................................... 531
7.1 Introduction ..................................................................................... 531
7.2 Position in Queensland ................................................................. 532
7.3 Addressing the risk of corruption .................................................. 532
7.4 Conclusions ..................................................................................... 536

Chapter 8 An organised crime specific offence / proceeds of crime .................................................................................... 539
8.1 Introduction ..................................................................................... 539
8.2 Organised crime specific offence .................................................... 539
  8.2.1 Queensland 539
  8.2.2 New Zealand 541
  8.2.3 New South Wales 544
  8.2.4 Western Australia 547
  8.2.5 South Australia 548
  8.2.6 Canada 548
8.3 Observations .................................................................................... 549
8.4 Proceeds of crime ........................................................................... 551

Appendices.......................................................................................... 555
Appendix 1 .......................................................................................... 555
Appendix 2 .......................................................................................... 558
Appendix 3 .......................................................................................... 561
Appendix 4 .......................................................................................... 562
Appendix 5 .......................................................................................... 564
Foreword

Many commissions of inquiry are asked to examine and report upon specific events or entities. This Commission’s task was quite different: the Terms of Reference required me to review the broad topic of organised crime in Queensland.

The Terms of Reference set out selected types of crime for the Commission’s particular emphasis. These areas—illicit drugs, child sex crimes, financial crimes, money laundering, and corruption—formed the direction of the Commission’s research and investigations. The chapters of this report reflect that focus.

As required, the Commission’s attention and recommendations concentrate on the impacts of such crime, the adequacy of the current government and law enforcement response, and the ways in which organised crime might be better addressed in the future.

During the Commission’s consultations it became clear to me that these areas of focus are also those of greatest importance to government and law enforcement agencies. It is my hope that the recommendations contained in this report will be well-received by these agencies and will assist them in performing their vital work.

The Commission sought to consult with all relevant State and Commonwealth agencies. I am grateful for the assistance and cooperation provided by these agencies, including the provision of a wealth of material that was essential to the Inquiry’s operation.

A number of individuals who had been directly affected by organised crime came forward and spoke to the Commission of their experiences. I would like to thank those who did so; the work of the Commission was significantly enhanced by these contributions.

The Commission gathered an enormous volume of material, through interviews, requests for documents, research and consultation with stakeholders. Compiling and analysing this material was only possible through the dedication and energetic work performed by counsel assisting and the staff of the Commission.

I want to thank counsel assisting, Michael Copley QC, Julie Sharp and Penny White who led a committed and talented team of lawyers during the six months of the Inquiry. The names of the Commission staff appear in Appendix 4.

It is a testament to the achievements of counsel assisting and staff that this lengthy and detailed report was delivered within the timeframe set by the Order in Council.

My particular thanks must also go to the Executive Director of the Commission, Louise Shephard. She took on the enormous dual roles of overseeing the efficient day to day operations of the Commission while simultaneously taking a proactive and hands-on role in shaping the content of this report.

Her administrative team ensured the smooth running of the many behind-the-scenes, but nevertheless essential, jobs including document management and liaison with outside entities.

It would be remiss of me not to specifically mention Detective Inspector Peter Brewer, whose insight into investigative methods and personal interaction with a number of persons who made submissions to the Commission has been invaluable.

There is no doubt that organised crime, in its various forms, will continue to pose a challenge to our society, government and law enforcement agencies. However, it is my hope that the findings and recommendations contained in this report will help to identify and prioritise areas of particular concern to the State and its citizens, and to provide appropriate deterrents to those who would engage in such deplorable and antisocial behaviours.

M. J. Byrne QC
Commissioner
Executive summary

The Commission commenced on 1 May 2015, by Commissions of Inquiry Order (No. 1) 2015, to make inquiry into the extent and nature of organised crime in Queensland and its economic and societal impacts.

The otherwise very broad nature of such an inquiry was somewhat narrowed by the Terms of Reference within the Order in Council, which focused the Commission on four key areas:

- the major illicit drug and/or precursor markets
- online child sex offending, including the child exploitation material market
- financial crimes, primarily investment/financial market fraud and financial data theft
- the relationship between organised crime and corruption in Queensland.

The Commission was also required to investigate the extent to which organised crime groups use various enabling mechanisms or services: in particular, money laundering, cyber and technology-enabled crime, identity crime, professional facilitators, violence and extortion.

In carrying out the Inquiry, the Commission was to examine the adequacy and appropriateness of current responses to organised crime by law enforcement, intelligence, and prosecution agencies, as well as the adequacy of legislation and of the resources available to such agencies.

The six-month timeframe given for the Inquiry was limited, given the areas required to be examined.

Outlaw motorcycle gangs

In embarking on the Inquiry the Commission was conscious that it was doing so in the shadow of the preceding 18 months of controversy regarding the former Queensland Government’s ‘crackdown’ on outlaw motorcycle gangs. The Commission was aware that the current Government intended to establish a special taskforce to review the 2013 suite of laws aimed at criminal groups, in particular, outlaw motorcycle gangs, and indeed the taskforce commenced in June 2015.

While the Commission therefore did not review the 2013 laws, it did endeavour to examine the presence of outlaw motorcycle gangs in organised crime. The Commission learned that outlaw motorcycle gangs play a major role in illicit drug markets in Queensland and are also involved in other illicit activity. Outlaw motorcycle gangs are increasingly exploiting their domestic and international connections, and using violence to extort money and assets from legitimate business owners, non-affiliated drug dealers, rival gangs and people operating in gang territory.

However, when considering the extreme legislation introduced by the former Government and the significant extra funding that was granted to the Queensland Police Service (QPS) ($14.2 million over two years) and the Crime and Corruption Commission (CCC) ($6.7 million over four years) to target outlaw motorcycle gangs, it is revealing to note that in the 21 month period from 1 October 2013 to 30 June 2015, outlaw motorcycle gang members accounted for only 0.52 per cent of criminal activity in Queensland.

While the Commission acknowledges that the CCC has fruitfully used its extra resources and enhanced intelligence function hearings (enhanced by the 2013 laws) to gather information on outlaw motorcycle gangs which has been of intelligence, tactical and strategic value, the Commission was concerned to learn that the heavy focus on outlaw motorcycle gangs has meant the CCC has lost visibility of other areas of organised crime active in Queensland.

Further, the evidence before the Commission suggests that the focus upon—and resources solely dedicated to—the threat of outlaw motorcycle gangs by the QPS, has meant that other types of organised crime have not been able to be appropriately investigated. This finding is outlined in the chapter on financial crimes (Chapter 5).
The Commission has recommended that the CCC extend the focus of its intelligence and research functions beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland. Likewise, the QPS should extend the focus of its policing strategies.

Illicit drug markets

With regards to the illicit drug markets, the Terms of Reference required the Commission to have particular regard to methylamphetamine, cocaine, heroin, drug analogues and new psychoactive substances, 3,4 – Methylenedioxymethamphetamine (MDMA/‘ecstasy’) and cannabis.

The Commission learned that illicit drug markets remain the most prominent and visible form of organised crime activity in Queensland. As at June 2015, indicative figures drawn from QPS intelligence revealed that 76 per cent of identified Queensland organised crime networks are involved in the illicit drug market, with 51 per cent linked to methylamphetamine, 30 per cent to cannabis and 12 per cent to MDMA/‘ecstasy’. Over one-third of organised crime networks linked to the illicit drug trade are involved with multiple drug types.

The Commission concluded that the legislation and resources available to law enforcement, criminal intelligence, and prosecution agencies in Queensland to prevent and effectively investigate and prosecute organised criminal activity in the illicit drug markets are generally adequate.

However, the Commission has recommended amendments to the Drugs Misuse Act 1986 and the Drugs Misuse Regulation 1987 to provide for a readily transparent and discernable penalty regime, which may have a greater deterrent effect on those who would use, or deal in, illicit drugs.

The methylamphetamine market poses the greatest threat to Queensland because of its prevalence across the state, the harm it causes, and the strong presence of organised crime in this market.

Mirroring the national trend, the growth in the use of crystal methylamphetamine (ice) has dramatically increased in Queensland. Ice has a significantly higher level of purity than traditional methylamphetamine. Its use has resulted in fatalities, is associated with aggression and violence, and is highly addictive.

The ice epidemic is a national issue and in early 2015 the Commonwealth Government announced the intention to develop the National Ice Action Strategy. To develop and implement this strategy, the National Ice Taskforce was established. An interim report of the taskforce recommended the establishment of a hotline to encourage community members to provide law enforcement with information concerning those who deal in ice.

The ‘dob-in-a-dealer’ telephone hotline has the potential to generate significant information and intelligence for Queensland police. However, the Commission is aware that the State Drug Squad is already using all resources available to it to action intelligence that it receives. The QPS must ensure that there are sufficient resources in place to deal with the additional workload generated by the new hotline.

For 2013–2014, Queensland had the highest number of detected clandestine drug laboratories in Australia, accounting for 45.8 per cent of the country’s total number of detected labs. Of those detected, 270 were used for the production of amphetamine-type stimulants.

Pseudoephedrine remains the most commonly used ingredient in the making of methylamphetamine and investigations suggest that pharmacists—specifically those who have poor prescribing practices and prescribe (knowingly or otherwise) larger-than-required quantities of pseudoephedrine—are the main source of the ingredient.

Pharmacists are heavily regulated, particularly with regard to the dispensing of pseudoephedrine. The majority of pharmacists in Queensland voluntarily use Project STOP, an online tool which tracks pseudoephedrine sales in real time. Project STOP is viewed as a critical initiative as its roll-out has had a significant impact on the ability of criminals to obtain pseudoephedrine from pharmacists. The Commission recommends that use of Project STOP should be mandatory for all Queensland pharmacies and pharmacists dispensing
pseudoephedrine-based products. The Commission notes that the associated costs are modest: a $300 annual fee for non-Pharmacy Guild members, and, if the pharmacist is a guild member, the program is free.

Drug analogues and new psychoactive substances have been increasing in global popularity since the mid-2000s: often advertised as legal alternatives to traditional illicit drugs such as heroin, MDMA/’ecstasy’, cannabis, LSD and amphetamine.

With some exceptions, drug analogues first emerged on the Queensland market in 2007 and have exploded since then in the number and variety available. Although illegal in Queensland, drug analogues are accessible over the Internet and have recently been available over the counter at adult stores, drug paraphernalia stores and ‘legal high’ stores.

However, these substances are dangerous, with their use associated with severe effects, serious illness and fatalities. The active ingredients in such substances are often unknown and untested on humans. Drug analogues can be inconsistent in potency across batches and are often more potent than the drug they are intended to mimic.

While the drug analogue market is not dominated by organised crime groups, such groups are becoming more involved in their importation and distribution. The Internet is one of the main sources of supply for drug analogues to users in Australia and in Queensland there are increasing networks of persons buying synthetic drugs in bulk online for on-sale.

Successive Queensland Governments have been alert to the drug analogue issue and have attempted to address the problem by specifically prohibiting substances once identified. However, the legislature cannot keep pace with the rate new substances are emerging on the market. While the definition of ‘dangerous drug’ in the Drugs Misuse Act has been extended to include analogues of scheduled substances, proving that a substance has a substantially similar affect to a prohibited drug can be difficult in the case of novel substances. The Commission has recommended that the extended definition of the term ‘dangerous drug’ within the Drugs Misuse Act (paragraph (c) (i), (ii) and (iii)) – should be reviewed to determine whether the definition effectively facilitates the successful prosecution of the unlawful possession of, and dealing in, drug analogues.

Cannabis is the most commonly used illicit drug throughout the world, with Australian use of the drug higher than the global average. This position is mirrored in Queensland, where cannabis is the illicit drug of choice. The National Drug Strategy Household Survey in 2013 indicated that 11.1 per cent of Queenslanders aged 14 years or older had used cannabis in the previous 12 months.

Although its common use indicates a perception that the drug is ‘harmless’, this is not the case and the use of the drug places social and economic (particularly health care sector) burdens on the state.

Organised crime groups, in particular family groups, are clearly present in the cannabis market, cultivating both bush and hydroponic cannabis plants, or transporting cannabis into Queensland from other states. Hydroponically grown cannabis is the dominant form available in the local market and because it is grown in a controlled environment it tends to be of a more consistent and higher potency.

In Queensland, the sale and purchase of hydroponic equipment, used to cultivate indoor cannabis, is not subject to the same regulation that applies to the sale and purchase of laboratory equipment, used to unlawfully produce synthetic dangerous drugs and drug analogues. Importantly, a person who supplies laboratory equipment to another must obtain certain information from that other person, including proof of identity and the person’s address, and maintain certain details of the transaction. This information, referred to as an end user declaration, must then be provided to police.

The Commission is of the view that extending the end user declaration scheme in Queensland to hydroponic equipment has the potential to prevent the misapplication of such equipment. However, hydroponic equipment is used by a large number of industries throughout Queensland for legitimate purposes. The Commission has recommended that the Queensland Government consider amending the Drugs Misuse Act
and Drugs Misuse Regulation to extend the end user declaration scheme to hydroponic equipment. It is the expectation of the Commission that such consideration will include extensive industry consultation.

The Darknet is becoming increasingly popular as a low-risk environment for individuals and organised crime groups to purchase and sell illicit drugs. The anonymity offered by encryption-based services and supplying via the post provides protection for offenders. The sale of drugs online through social media platforms and chat rooms is also increasing in popularity.

Given the social and economic impacts of drug crime and that dealing in dangerous drugs over the Internet is an increasing trend, the Commission recommends that the QPS invest further resources into the monitoring of such online illicit activity. Further, while Queensland’s dangerous drug offences carry strong penalties, the Commission has recommended that higher maximum penalties should apply where the drugs are procured or supplied using the Internet.

### Online child sex offending and child exploitation material

Online child sex offending and the child exploitation material market is fast evolving, alongside advances in technology.

The cyber environment provides a relatively anonymous platform from which predators can access countless children. Often posing as children, offenders infiltrate online chat rooms, instant messaging services, and social networking sites in the attempt to engage young people for various deviant purposes. Tactics aim to disinhibit children and form a rapport that encourages them to share personal information and ultimately engage in the predator’s sexual fantasy. That engagement might end with sexually explicit dialogue—or the provision of images or videos—or it might escalate to a meeting where the goal is contact offending.

The Internet has provided an environment for the proliferation of child exploitation material and the creation of an expanding market for its consumption. Offenders in this area are becoming more sophisticated and technically adept, and are often early adopters of new technologies.

The Commission was told of the alarming demand for increasingly depraved material involving the abuse of children. Membership of some highly networked child exploitation material sites requires the production and uploading of new material – on a regular basis – increasing the demand for child victims.

Networks that are used to share child exploitation material vary in size and sophistication. Peer-to-peer platforms allow loosely connected users to grow their own collections and share with others. At the other end of the scale, enormous, hierarchical networks have been formed through the development of organised and sophisticated sites protected by the anonymity of the Darknet.

The Commission learned that networks of offenders involved in online child sex offending are currently operating in Queensland and that there are significant numbers of Queensland children caught up in these enterprises.

The QPS (in particular, Taskforce Argos) is a world leader in policing online child sex offending. It has forged relationships with international counterparts and has developed skill sets vital to tackling this global problem. Importantly, Taskforce Argos prioritises victim identification, and has been successful in removing many children from harm as a result.

The legislative framework in Queensland, for the most part, adequately covers the range of offending in the area of online child sex offending, including the child exploitation material market. Amendments to the Commonwealth Criminal Code in 2013 ensures that aggravated penalties apply to network offending. The Commission did, however, identify a number of areas that might be strengthened by legislative change.

The Commission has recommended increasing the maximum penalties for the offences of involving a child in making child exploitation material (section 228A of the Criminal Code) and making child exploitation material (section 228B of the Criminal Code) from 14 years imprisonment to 20 years imprisonment.
Given what the Commission has learned about the market becoming increasingly depraved and voracious for new material, it is the Commission’s view that it is appropriate to reintroduce the penalty distinction between offenders who make child exploitation material and those who possess or distribute it. The offences of distributing (section 228C of the Criminal Code) and possessing (section 228D of the Criminal Code) child exploitation material should continue to attract the current maximum penalty of 14 years imprisonment.

The Commission has recommended that higher maximum penalties should apply for offenders who engage in the child exploitation material market using the Darknet or other anonymising service.

The use of the Darknet, as well as other proxies and anonymising services, makes detection and investigation of child exploitation material offenders much more difficult. Further, the nature of offending within these hidden networks is generally more serious and more likely fall into the category of organised crime. The Darknet child exploitation material sites often require members to produce new material, and some offer on-demand abuse of children.

For the offences of involving a child in making child exploitation material (section 228A) and making child exploitation material (section 228B), the circumstance of aggravation would increase the maximum penalty from 20 years to 25 years imprisonment. An increased maximum penalty of 20 years imprisonment would apply for the offences of distributing (section 228C) and possessing (section 228D) child exploitation material.

A gap in the legislative framework exists in respect of administrators of child exploitation websites, where dealing in the child exploitation material cannot be proved, and in respect of those who encourage others to engage in the child exploitation material market and those who provide advice on avoiding detection by law enforcement agencies. The ‘party’ provisions in the Criminal Code have limited use in such circumstances.

To address this gap the Commission has recommended the creation of new offences to be inserted into the Criminal Code, possibly modelled on similar provisions existing in the Victorian Crimes Act 1958.

A vulnerability in the capacity of law enforcement to access electronically stored data that is protected by passwords and encryption tools must be rectified.

Offenders engaged in the child exploitation material market use encryption, anonymous proxies and kill switches to avoid detection. While Queensland police can apply to a magistrate or judge for an order, to be included in a search warrant, for a suspect to provide police with necessary passwords or other information to gain access to stored information, failure to do so carries a toothless maximum penalty of 12 months imprisonment. Online child sex offenders are liable to a far greater maximum penalty if convicted, than the 12 months imprisonment for refusing to comply with a warrant.

The CCC is hampered in its investigations because it has no legislative ability to seek an order requiring a suspect to assist investigators in accessing stored information. The Commission has recommended amendments to enable the CCC to seek such orders from an issuer of a search warrant.

Further, the Commission has recommended the creation of a specific offence applying to the failure of a person to comply with an order in a search warrant about information necessary to access electronically stored information. The offence should carry a maximum penalty of five years imprisonment, increasing to seven years when the offender was in possession of child exploitation material at the time the search warrant was executed.

Concerns were expressed to the Commission from law enforcement and prosecution agencies regarding the ‘Oliver scale’, a child exploitation material classification system routinely used by Queensland courts in sentencing offenders. The Oliver scales allows courts to sentence offenders without having to review a sample of the evidence to assess its seriousness.

The concerns relate to the enormous amount of time it takes police officers, and civilians in the employ of law enforcement agencies, to assign one of six classifications to each of the millions of images found in the possession of offenders. For law enforcement agencies, that task takes resources away from victim identification and the priority of rescuing those children from further harm. For the Office of the Director of
Public Prosecutions, the time taken by law enforcement to classify the images and video files often means delays in prosecuting offenders.

The Commission’s position is that the Oliver scale should be maintained but acknowledges that suggested reform such as moving to a three category system or utilising random sampling have merit and deserve to be appropriately reviewed and considered. The limited timeframe for this Inquiry did not allow the Commission to undertake such a review, however, the Commission has recommended such a review to the proposed new Sentencing Advisory Council.

**Financial crimes**

The consequences of a blinkered approach to combating organised crime in Queensland—in recent times on account of the heavy focus on outlaw motorcycle gangs—were brought into stark relief in the Commission’s inquiry into financial crimes.

The Terms of Reference required the Commission to consider the nature and extent, and economic and societal impacts of organised crime in Queensland in the area of financial crime, primarily investment and financial market fraud and financial data theft.

It was in the area of investment fraud that the Commission discovered a serious, organised crime problem that has been allowed to flourish in Queensland, and which remains current. Law enforcement officers variously described the problem as ‘out-of-control’ and an ‘epidemic’.

The Commission learned that cold-call investment frauds (also known as boiler rooms) have been operating on the Gold Coast for many years. These types of investment frauds are sophisticated and organised, using complex business structures, slick marketing material and aggressive telemarketing tactics to create a veneer of legitimacy. In this way criminal syndicates have fleeced thousands of Australians of millions of dollars of savings.

The impacts of such losses are immense. Victims have been known to suffer significantly as a result of their (often financially devastating) economic loss. Anxiety and depression, in extreme cases leading to suicide, are some of the by-products of this type of organised crime.

The QPS, in particular the Fraud and Cyber Crime Group (formerly the Fraud and Corporate Crime Group), has never been properly resourced to effectively deal with the burgeoning problem. Compounding the lack of resources are a number of other factors, including the complexity of the frauds (and questions about whether they are in fact criminal frauds) and an attitude that complainants have failed to act in a financially responsible way.

The Commission held in camera hearings in respect of those issues against the background of specific complaints that had been made about the failure of the QPS to adequately deal with the problem of boiler-room frauds proliferating on the Gold Coast. The hearings were not conducted in public given the restrictions rightly imposed on the Commission by the Terms of Reference. Despite that, to the extent allowed, the Commission has reported on the information and evidence received.

The evidence heard in the course of the hearings, as well as other documentary evidence and submissions, led the Commission to make a finding that the QPS has failed to adequately respond to complaints from persons claiming to have been defrauded by people operating boiler-rooms. This failure is largely attributable to inadequate resourcing, and likely influenced by an attitude that the complainants have failed to exercise due diligence concerning their own finances.

It became clear that because policing priority must be given to matters of public safety, and other perceived imperatives (including to resource Taskforce Maxima and to investigate frauds against the government), the Fraud and Cyber Crime Group have often been left, depleted of staff, to ‘make do’ with what resources are left. The Commission has made recommendations that it is hoped will address that resourcing problem. Since it is well-known that there is a significant organised crime problem within the ‘brief’ of the Fraud and Cybercrime Group, it is imperative that that group (and others that might assist in the task) be properly
Executive Summary

resourced to combat cold-call investment frauds operating in Queensland. To that end, the Commission has recommended that a taskforce be established.

In addition to proper resourcing, the Commission has recommended changes in the way the QPS assess complaints regarding suspected boiler rooms, suggesting that some assistance might be drawn from the expertise of the Office of the Director of Public Prosecutions. Cold-call investment frauds should be given priority in respect of intelligence collection, and education in ‘economic crime’ for new recruits and detectives (and refresher training for existing detectives) is also recommended.

Aside from investment frauds, a range of other types of financial crime were considered in accordance with the Terms of Reference.

Financial data theft and the related ‘key enabler’, identity crime, are often inextricably linked and were found to be prevalent notwithstanding under-reporting. In respect of just one type of financial data theft—card-not-present-fraud—the Commission learned of staggering losses, in the order of $299 million, reported by the Australian Payments Clearing Association in 2014.

Various other types of financial data theft, including skimming, phishing (and related frauds) and the use of hacking, malware and ransomware by criminal syndicates, were also examined. While the Queensland community is no doubt as vulnerable to those types of crimes as most other communities, the Commission was informed that the syndicates committing the crimes are more often located off-shore.

Scams targeting the Queensland community, including advance-fee frauds (often attributed to Nigerian syndicates) and the increasingly prevalent and damaging romance scams, also continue to affect the community. The Commission learned that efforts have been made by the QPS and other agencies to educate the public regarding these scams in an effort to prevent people from falling prey. Prevention is particularly important in respect of these types of financial crime given the challenges in locating overseas offenders and bringing them to justice.

Cyber and technology-enabled crime, identity crime and professional facilitators are known to enable financial crimes. The prevalence of cybercrime in this era of increasingly sophisticated technology has led to an increased focus by law enforcement and intelligence agencies around the world. In Australia, the National Plan to Combat Cybercrime has led to the establishment of the Australian Online Reporting Network (ACORN).

ACORN is a national policing initiative, providing an online, secure portal for members of the public to report cybercrime. ACORN also provides information about how to recognise scams and gives advice to those who have become victims. The alarming number of ACORN reports being referred to the QPS indicates the effectiveness of this initiative, but also the extent of the impact of cybercrime on Queensland citizens. The Commission has recommended that the Fraud and Cybercrime Group be adequately resourced to deal with the unexpected volume of referrals from ACORN.

A recurring theme in relation to the involvement of professional facilitators in enabling organised crime was the absence of obligations for lawyers, accountants and real estate agents under the Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) regime. The risk of real estate agents, and others involved in property transactions, becoming unwitting facilitators of real estate fraud (through the use of false or stolen identities) has led the Commission to recommend that visual verification of identification requirements be included in guidelines for property agents, mortgagees and mortgage transferees.

The adequacy of the legislative framework comprised of the Criminal Code (Qld) (dealing with fraud and fraud-related offences) and the Criminal Proceeds Confiscation Act 2002 (Qld) and the Criminal Code (Cth) (dealing with money laundering) was examined in accordance with the Terms of Reference.

The Commission has made recommendations for a range of legislative changes to the Criminal Code which are aimed at providing stronger sentencing options for courts sentencing offenders for fraud, including...
heavier penalties for circumstances of aggravation which would include frauds committed in the organised crime context of cold-call investment frauds, and for all frauds involving over $100,000.

The Commission has also recommended strengthening penalties for obtaining or dealing with identification information, proscribed by section 408D of the Criminal Code. That would bring the penalties in line with those that apply to fraud under section 408C of the Code and recognise that identity crime is now known to be a prevalent crime in its own right, as well as an enabler of other types of crime, including organised crime.

Further, the Commission has made recommendations aimed to assist police in their investigations into financial crimes (by making it simpler to obtain production orders for financial records), and for victims to recover lost money from funds forfeited under the Criminal Proceeds Confiscation Act.

Money laundering

Money laundering to ‘clean’ illicit funds is a significant global issue. Australia is one of the largest financial markets in the Asia-Pacific region, which makes it very susceptible to money laundering.

In Queensland, the requirement to obtain the consent of the Attorney-General prior to a person being charged with the Queensland offence of money laundering under the Criminal Proceeds Confiscation Act 2002 (Qld) is an issue that should be addressed immediately. The practical effect of the consent requirement is that the QPS is electing to charge people with the Commonwealth offence over the Queensland offence. The Commission can see no reasonable rationale for the requirement for ministerial consent.

Corruption

The Commission was required by the Terms of Reference to consider and report on the relationship between organised crime and corruption in Queensland. In the context of this Inquiry, the Commission interpreted that requirement as referring to public sector corruption—an issue that is the subject of much analysis and focus by law enforcement and academics around the world when considering activities and links to organised crime.

The Commission did not discover any evidence of—or receive any reliable information to suggest—corruption of public officials by persons associated with organised crime or to suggest that organised crime entities are attempting to proactively infiltrate government departments or agencies for the purpose of furthering criminal activity.

While there is no evidence in Queensland of a significant corruption problem, common sense dictates that the potential for such conduct is a risk to government, and that proactive measures should be taken to minimise such risks. The focus should be on law enforcement agencies, and public sector agencies that control or regulate industries or activities, and which issue identification documents.

The Commission has recommended the introduction of mandatory declarable associations policies in identified high-risk agencies or high-risk business units within agencies. It is the Commission’s view that such mandatory declaration policies will increase awareness across the Queensland public sector of the risk posed to public officers of being targeted and groomed by organised crime groups.
Recommendations

The Queensland Organised Crime Commission of Inquiry recommends that:

Chapter 2 Outlaw motorcycle gangs

2.1 The Crime and Corruption Commission extend the focus of its intelligence and research functions beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland.

2.2 The Queensland Police Service extend the focus of its policing strategies beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland.

Chapter 3 The illicit drug market

3.1 The Queensland Police Service ensure that there are sufficient resources in place to deal with the additional workload generated by the Dob-in-a-Dealer telephone hotline, a Federal Government initiative aimed to attack the ice epidemic.

3.2 The Queensland Government review the extended definition of the term ‘dangerous drug’ within the Drugs Misuse Act 1986—that is, limb (c) (i), (ii), and (iii)—to determine whether the definition effectively facilitates the successful prosecution of the unlawful possession of, and dealing in, drug analogues. In particular, such a review should examine alternative approaches in other jurisdictions.

3.3 The Queensland Police Service consider increasing the number of operations targeting drug analogues in mining regions in Queensland, given the prevalence of drug analogues in these regions and the apparent inability of mining companies to test for such ever-evolving drugs.

3.4 The Queensland Government amend the Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987 to omit the current distinction between types of dangerous drugs by including all dangerous drugs in the one Schedule. The maximum penalties that apply for offences relating to current Schedule 1 dangerous drugs should be retained and applied to all dangerous drugs. The quantities specified in Schedules 3 and 4 should be retained but moved to be included in the dangerous drug Schedule for ease of reference. Consequential amendments should be made to ensure appropriate offending can still be dealt with summarily.

3.5 The Queensland Government consider amending the Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987 to extend the current end user declaration scheme to hydroponic equipment.

3.6 The Queensland Police Service invest further resources into the area of online drug offending. In particular, additional police officers with sufficient training and expertise in cybercrime, be tasked to monitor online activity, with a view to infiltrating the activities of those purchasing and selling drugs over the Internet.

3.7 The Queensland Government amend the Drugs Misuse Act 1986 to apply aggravated penalties to the offences of possessing, supplying and trafficking in dangerous drugs where such conduct is facilitated by the Internet. The circumstance of aggravation would attract an additional five years. This will increase the maximum penalties to 20 years, 25 years, and life imprisonment.

3.8 The Queensland Government legislate to make Project STOP mandatory for all pharmacies and pharmacists dispensing pseudoephedrine in Queensland. This may be achieved by inserting a provision in the Health (Drugs and Poisons) Regulation 1996.

3.9 The Queensland Government amend section 590AB (Disclosure obligation) of the Criminal Code to require all documents to be provided in non-electronic form, as well as in electronic form if the latter is available.
Chapter 4 Online child sexual offending and child exploitation material

4.1 The Queensland Government proposed independent crime statistical body, once established, prioritise the collection and analysis of data relevant to organised crime in Queensland.

4.2 The Office of the Director of Public Prosecutions considers implementing guidelines similar to the Commonwealth Director of Public Prosecutions’ Online child exploitation conduct of matters guideline, particularly as it relates to limiting the time a member of staff is exposed to child exploitation material in any one sitting.

4.3 Legal Aid Queensland considers implementing guidelines similar to the Commonwealth Director of Public Prosecutions’ Online child exploitation conduct of matters guideline, particularly as it relates to limiting the time a member of staff is exposed to child exploitation material in any one sitting, for the protection of its officers (and preferred suppliers) who are exposed to child exploitation material.

4.4 The Queensland Government amend the Criminal Code to include provisions that would criminalise the contribution of administrators of child exploitation websites, as well as those who encourage their use and provide advice to avoid detection and add to the proliferation of child exploitation material online. In developing the new provisions regard should be had to sections 70AAAB, 70AAAC and 70AAD of the Crimes Act 1958 (Vic).

4.5 The Queensland Government amend the Criminal Code by increasing the maximum penalty for sections 228A (Involving child in making child exploitation material) and 228B (Making child exploitation material) from 14 years to 20 years imprisonment.

4.6 The Queensland Government amend the Criminal Code to include a circumstance of aggravation for each of the child exploitation material-related offences in sections 228A, 228B, 228C and 228D. The circumstances of aggravation would apply to any new offence (in relation to administrators of child exploitation websites, those who encourage their use and those who provide advice to avoid detection) enacted in accordance with recommendation 4.4.

4.7 The Queensland Government amend section 154 (Order in search warrant about information necessary to access information stored electronically) of the Police Powers and Responsibilities Act 2000 so that:

- ‘stored information’ includes information accessible by a computer or storage device (for example from a ‘cloud’ storage service); and
- an application for another order may be made after the seizure of a computer or storage device; and
- an order may contain conditions for the provision of access information at some future time when the computer or storage device is not on the premises.

In developing the amendments regard should be had to section 465AA of the Crimes Act 1958 (Vic).
Amendments to the Crime and Corruption Act 2001

4.8 The Queensland Government amend Chapter 3, Part 2 (Search warrants generally) of the Crime and Corruption Act 2001 to include a provision allowing for the issuer of a search warrant to make orders about information necessary to access information, in the same, or similar, terms as section 154 of the Police Powers and Responsibilities Act, as amended in accordance with recommendation 4.7.

A consequential amendment might also be made to provide that a failure to comply with such an order may be dealt with under the new offence provision in the Criminal Code recommended in 4.9, below.

Amendments to the Criminal Code

4.9 The Queensland Government amend the Criminal Code to insert a new offence of failing to comply with an order in a search warrant about information necessary to access information stored electronically (whether made under the Police Powers and Responsibilities Act 2000 or the Crime and Corruption Act 2001). The offence would be an indictable offence, and carry a maximum penalty of five years imprisonment.

The new offence would include a circumstance of aggravation, increasing the maximum penalty to seven years imprisonment, when the specified person is in possession of child exploitation material at the time the search warrant is executed.

Section 552A of the Criminal Code should be amended to provide that the new offence may be heard summarily on the prosecution election.

4.10 The Queensland Attorney-General seek to include legislative and other measures apt to block or remove child exploitation material on to the 2015–2016 agenda for the Law, Crime and Community Safety Council.

4.11 The Queensland Government proposed Sentencing Advisory Council, once established, as a matter of priority, review the use of the current ‘Oliver scale’ classification system, other classification options, and the merits of using random sampling, in the sentencing process.

4.12 The Queensland Police Service seek to execute and implement, as a matter of priority, the Joint Anti-Child Exploitation Team Memorandum of Understanding.

4.13 The Queensland Police Service and the Crime and Corruption Commission prioritise the implementation of the Kent Internet Risk Assessment Tool.

4.14 The Queensland Police Service and Crime and Corruption Commission be properly resourced, including with technical staff and analysts, to undertake a ‘blitz’ and tackle to a greater degree known Queensland-based offenders sharing child exploitation material on peer-to-peer platforms.

Chapter 5 Financial crimes

5.1 The Office of Fair Trading develop and publish ‘best practice guidelines’ for property agents, including the visual verification of identity.

5.2 The Queensland Government ensure that the Land Title Practice Manual includes a requirement for visual verification of identity before a mortgagee or mortgage transferee is deemed to have taken ‘reasonable steps’ under sections 11A and 11B of the Land Title Act 1994.

5.3 The Queensland Government amend section 408C (Fraud) of the Criminal Code by increasing the maximum penalty for aggravated fraud in subsection (2) to 14 years imprisonment.

5.4 The Queensland Government amend section 408C (Fraud) of the Criminal Code by inserting an additional circumstance of aggravation, to apply if the property, or the yield to the offender from the dishonesty, or the detriment caused, is of a value of $100,000 or more.

In that case, the maximum penalty would be 20 years imprisonment.
5.5 The Queensland Government amend section 408C (Fraud) of the Criminal Code by inserting an additional circumstance of aggravation, carrying a maximum penalty of 20 years imprisonment, where the fraudulent conduct involved the planned and systematic targeting of the public.

5.6 The Queensland Government further amend section 408D (Obtaining or dealing with identification information) of the Criminal Code by extending the ambit of the circumstance of aggravation in subsection (1AA) as follows:

(1AA) If the person obtaining or dealing with the identification information supplies it for the benefit of a criminal organisation, or 2 or more members of a criminal organisation, or at the direction of, or in association with, a criminal organisation, the person is liable to ....

5.7 The Queensland Government amend section 408D (Obtaining or dealing with identification information) of the Criminal Code to increase the maximum penalties as follows:

(1) 5 years imprisonment  
(1AA) 14 years imprisonment  
(1A) 5 years imprisonment.

5.8 The Queensland Government amend Chapter 7, Part 4 of the Police Powers and Responsibilities Act 2000 to allow production notices to be issued by a Justice of the Peace or a Magistrate.

5.9 The Queensland Government consider establishing a scheme to allow the victims of serious frauds to apply for compensation from property forfeited to the State under Chapter 3 of the Criminal Proceeds Confiscation Act 2002.

5.10 The Queensland Police Service prioritise cold call investment frauds for intelligence collection. The Queensland Police Service State Intelligence Unit be properly resourced to produce a detailed intelligence report regarding cold-call investment frauds operating in Queensland.

5.11 The Queensland Police Service Fraud and Cyber Crime Group be appropriately resourced to deal with the much higher than expected volume of complaints referred to the police through the Australian Cybercrime Online Reporting Network.

5.12 The Queensland Police Service ensure by appropriate means that all operational police officers are aware that:

- It is not appropriate to have reference to section 3.4.3 (Factors to consider when deciding to prosecute) of the Queensland Police Service Operational Procedures manual when assessing whether a complainant is civil or criminal in nature; in determining whether it will be investigated by the Queensland Police Service, and if so, what priority it is to be given.
- The law relating to the element of dishonesty in section 408C of the Criminal Code has changed by virtue of the decision in R v Dillon; Ex parte Attorney-General (Qld) [2015] QCA 155.

5.13 The Queensland Police Service establish a dedicated taskforce, resourced by specialist investigators and other personnel, to address cold-call investment frauds.

5.14 The Queensland Police Service include the economic crime course in the curriculum for new recruits and for detective training. A refresher course should be developed and implemented for existing detectives.

5.15 The Office of the Director of Public Prosecutions and the Queensland Police Service develop a mechanism for collaboration between the two agencies in respect of assessing alleged frauds for criminality.
Chapter 6 Money laundering

6.1 The Queensland Government amend section 251 (Charging of money laundering) of the Criminal Proceeds Confiscation Act 2002, to remove the requirement for Attorney-General consent.

Chapter 7 Corruption

7.1 All Queensland Government departments and agencies undertake an audit to identify high-risk areas, in terms of information, assets, materials and functions.

Persons employed in those identified high-risk areas complete (and keep current) a statement of their declarable associations.

Chapter 8 An organised crime specific offence/proceeds of crime

8.1 The Queensland Government amend the Criminal Proceeds Confiscation Act 2002, so that the Crime and Corruption Commission administer the Chapter 3 scheme, and the Crime and Corruption Commission conduct all court proceedings under the Act.
The concept of ‘organised crime’ has its roots in the United States of America. Members of the Chicago Crime Commission—an organisation established in 1919 by businessmen, bankers and lawyers to lobby for criminal justice system changes addressing the Chicago crime problem—were the first to regularly use the term. The term was used in a broad sense to refer to a certain criminal class that could pursue crime as a business—that is, professional criminals.

During the Great Depression, the concept of organised crime changed to reference ‘gangsters and racketeers who were organised in gangs, syndicates and criminal organisations and followed big master criminals who functioned as powerful leaders of organised crime’. From the 1950s, the term became synonymous with the Mafia, and was a prominent feature of the criminal policy debate in the United States during the 1960s.

The concept and term has gained a global foothold, although there is no common definition of ‘organised crime’. Definitions vary among countries—and within a jurisdiction, different definitions may be used for different purposes. However, it is clear that the concept of organised crime has expanded beyond highly structured and hierarchical organisations, to encompass less-formal groups and undefined criminal networks.

In an Australian context, the public image of organised crime over the decades has been steeped in violence. The Melbourne gangland killings saw 36 members or associates from underworld groups killed during the 12-year period from 1998 to 2010. Outlaw motorcycle gangs have also had a high profile, due to events such as the Milperra Massacre in 1984, when a gun battle between the Comancheros and the Bandidos left seven dead—including a child.

Governments around the world have determined that organised crime necessitates specific legislative responses; traditional criminal offences are insufficient to disrupt criminal organisations. In 1970, the United States enacted the Racketeer Influenced and Corrupt Organizations Act, which provides for criminal sanctions and confiscation of proceeds of crime where prescribed crimes are committed as part of an enterprise.

Apart from legislation addressing asset forfeiture and money laundering, a number of jurisdictions, including some in Australia, have introduced specific offences that criminalise ‘participation’ in a criminal organisation. Other countries have introduced legislative schemes that allow for a group to be declared a criminal organisation, which then facilitates the making of prohibition and anti-association orders against its members and associates. A number of Australian states and territories—including Queensland—introduced such legislation in response to ongoing and escalating violence between outlaw motorcycle gang members in Sydney in 2008–2009.
1.1 The Commission of Inquiry

In response to public violence on 27 September 2013 between rival outlaw motorcycle gangs at Broadbeach, Queensland—and a subsequent violent incident between police and members of the Bandidos that same evening—the Newman Government announced its intention to ‘crackdown on criminal gangs’.

On 15 October 2013, the then-Government introduced a suite of legislation (referred to in this report as ‘the 2013 legislation’) into the Queensland Parliament. Despite the then-Opposition opposing the urgency motion, the suite of bills was declared urgent, and the parliamentary debate began hours after their introduction. The suite of bills passed in the early hours of the following morning. The speed with which the legislation was enacted—and the resulting lack of public scrutiny—drew criticism. Furthermore, the laws themselves have attracted significant publicity and controversy.

The 2013 legislation particularly focused on outlaw motorcycle gangs, and created new offences and aggravated offences under the Criminal Code. The legislation also changed bail laws, introduced minimum mandatory penalties, increased powers for law enforcement agencies, and introduced vetting in certain licensed industries. The package of reforms included the enactment of the Vicious Lawless Association Disestablishment Act 2013 (the VLAD Act), which provides a crushing mandatory cumulative sentencing regime for people who participate in the affairs of an association and commit declared offences for the purpose of, or in the course of, that participation.

The Queensland Government, while in Opposition, did not oppose the passage of the 2013 legislation; however, it made an election commitment during the 2015 State election campaign to establish a Commission of Inquiry into organised crime and to create a high-level taskforce to review the 2013 legislation.

The Commission was established by the Commissions of Inquiry Order (No. 1) 2015 to make full and careful inquiry into the nature, extent, and economic and societal impacts of organised crime in Queensland. The Commission commenced on 1 May 2015, and functioned with all the powers provided under the Commissions of Inquiry Act 1950. Mr Michael Byrne QC was appointed as Commissioner to lead the Inquiry. Mr Michael Copley QC was engaged as senior counsel assisting the Commission. Ms Julie Sharp and Ms Penny White were also engaged as counsel assisting. Staff of the Commission were drawn from the legal, policy, and policing fields. Appendix 2 outlines the establishment and operations of the Commission.

1.2 The scope of the Inquiry

The scope of the Commission’s inquiry and its timeframe for reporting are set out in the Terms of Reference, outlined in the Commissions of Inquiry Order (No. 1) 2015. The Terms of Reference required the Commission to examine the nature, extent and impacts of organised crime in a number of key areas:

- the major illicit drug and/or precursor markets
- online child sex offending, including the child exploitation material market
- financial crimes, primarily investment/financial market fraud and financial data theft
- the relationship between organised crime and corruption in Queensland.

The Commission was also required to investigate the extent to which organised crime groups use various enabling mechanisms or services—in particular, money laundering, cyber and technology-enabled crime, identity crime, professional facilitators, violence and extortion.

In carrying out the Inquiry, the Commission was to examine the adequacy and appropriateness of current responses to organised crime by law enforcement, intelligence, and prosecution agencies, as well as the adequacy of legislation and of the resources available to such agencies.

Ultimately, the Commission was required to identify high-risk organised crime threats and future trends, and to recommend priority areas of focus for government and law enforcement.
1.2.1 Exclusions

Paragraph 8 of the Terms of Reference provided that the Commission was not to have regard to any matter that was, at the time of the Inquiry, the subject of a judicial proceeding or a proceeding before an administrative tribunal or commission (including a tribunal or commission established under a Commonwealth law).

The Commission interpreted paragraph 8 of the Terms of Reference as excluding the Commission from examining and reporting on a current proceeding in a manner that would influence or jeopardise the proceeding. The Commission did not view paragraph 8 as a blanket prohibition on matters that had essentially concluded (apart from, for example, an appeal).

For the most part, current matters are not referred to in the report; however, there are examples in the report where reference is made to current matters where such reference is to publicly available information and where such referencing would not impact on the proceeding.

While paragraph 8 was an appropriate exclusion from the scope of the Inquiry, it proved to be very restrictive due to the lengthy timeframes that can apply to a criminal prosecution from commencement to finalisation—particularly for matters prosecuted on indictment.

The Terms of Reference also imposed reasonable limitations on the Commission with regards to the publication of certain information, to ensure that it did not publish details of intelligence-collection strategies and investigation methodologies or information concerning covert investigations.

1.2.2 Defining ‘organised crime’

There is no common definition of ‘organised crime’. Definitions vary among countries, and within one jurisdiction, different definitions may be used for different purposes. Queensland is no exception. It is, therefore, unsurprising that the Terms of Reference did not attempt to define the term ‘organised crime’, but rather allowed the Commission to determine its scope for the purpose of this Inquiry. That said, the Terms of Reference did partly define the term ‘organised crime’ by outlining the criminal activities and illicit markets that the Commission was to focus on.

The United Nations Convention Against Transnational Organized Crime (the UN Convention), Article 2, defines ‘organised criminal group’ as meaning:

- a structured group of three or more persons;
- existing for a period of time and acting in concert;
- with the aim of committing one or more serious crimes or offences (an offence punishable by at least four years imprisonment);
- in order to obtain, directly or indirectly, a financial or other material benefit.

The term ‘structured group’ is defined to mean:

- a group that is not randomly formed for the immediate commission of an offence;
- does not need to have formally defined roles for its members;
- does not need to have continuity of its membership;
- does not need to have a developed structure.

The UN Convention definition recognises that loose arrangements of people may fall within the ambit of an organised crime group—that is, groups assembled on a short-term basis for specific projects.

The Australian Crime Commission Act 2002 (Cth), section 4, defines ‘serious and organised crime’ to mean:

- a prescribed offence punishable by at least three years imprisonment or a ‘serious offence’ as defined by the Proceeds of Crime Act 2002 (Cth)
that involves two or more offenders
that involves substantial planning and organisation
that involves or ordinarily involves the use of sophisticated methods and techniques
that is committed or ordinarily committed in conjunction with other like offences.

Unlike the UN Convention definition, the Australian Crime Commission Act requires substantial planning and organisation, and contemplates a sophisticated modus operandi.

Within a Queensland context, the *Crime and Corruption Act 2001* (Qld) defines ‘organised crime’ to mean criminal activity that involves:

- indictable offences punishable on conviction by a term of imprisonment not less than seven years
- two or more persons
- substantial planning and organisation or systematic and continuing activity
- a purpose to obtain profit, gain power or influence.

The *Police Powers and Responsibilities Act 2000* (Qld) defines ‘organised crime’ to mean:

- an ongoing criminal enterprise
- to commit serious indictable offences
- in a systematic way
- involving a number of people
- involving substantial planning and organisation.

The Police Powers and Responsibilities Act definition may be viewed as unnecessarily restrictive in requiring proof that the organisation is an ongoing criminal enterprise. While the UN Convention definition excludes groups that are formed for the immediate commission of an offence, it does allow for loose arrangements of people assembled on a short-term basis for specific projects. The Crime and Corruption Act (Qld) definition does not require proof of systematic and continuing activity, if substantial planning and organisation is evident.

For the purpose of the Inquiry, the Commission considered a matter within scope if it involved criminal offences falling within the ambit of paragraph 3(b) of the Terms of Reference, committed by a number of people:

- involving substantial planning or continuing activity
- committed for financial gain and/or which may harm the welfare of the Queensland community, or
- if the offences are connected to the enabling activities outlined in paragraph 3(d) of the Terms of Reference.

The Commission also considered a matter within scope where the criminal offence did not fall within the ambit of paragraph 3(b) of the Terms of Reference, but nonetheless was significantly connected to the outlined enabling activities.

### 1.3 Process of the Inquiry

Paragraph 4 of the Terms of Reference required the Commission to gather information by calling on law enforcement, intelligence, and prosecution agencies, as well as academics and relevant industry, and by reviewing relevant literature and data. Paragraph 5 of the Terms of Reference allowed the Commission to have regard to the experiences of individuals and other entities directly or indirectly affected by organised crime.

The Commission obtained information by a range of methods. On 24 April 2015, a call for information was posted on the Commission’s website. Public notices appeared in *The Courier-Mail* and *The Australian* on 29 April 2015 and 2 May 2015.
In its first weeks of commencement, the Commission met with the following key stakeholders, inviting submissions from those agencies on the Terms of Reference:

- Queensland Police Service (QPS)
- Crime and Corruption Commission
- Director of Public Prosecutions
- Legal Aid Queensland
- Queensland Law Society
- Bar Association of Queensland
- Legal Services Commission Queensland
- Integrity Commissioner, Australian Commission for Law Enforcement Integrity.

The Commission also wrote to the following entities, alerting them to the Inquiry and inviting a submission:

- Queensland University of Technology
- University of Queensland
- Griffith University
- Bond University
- James Cook University
- University of Southern Queensland
- Pharmacy Board of Australia
- Association of Financial Advisors
- Australian Information Industry Association
- IT Queensland
- Australian Competition and Consumer Commission
- Institute of Public Accountants
- CPA Australia
- Chartered Accountants of Australia and New Zealand
- Real Estate Institute of Queensland
- Australian Crime Commission
- Australian Federal Police
- Together Queensland
- Queensland Police Union of Employees
- Queensland Council of Civil Liberties
- Queensland Police Commissioned Officers’ Union of Employees
- Dr Caitlin Byrne (Bond University)
- Mr Terry Goldsworthy (Bond University)
- Gold Coast Central Chamber of Commerce
- Mr Ken Gamble (private investigator).

The nature and subject matter of the Inquiry did not readily lend itself to public hearings. The majority of the submissions and information provided to the Commission were done so with reasonable requests for confidentiality.

The Commission relied on its powers under the Commissions of Inquiry Act 1950 to seek information and documents from organisations and individuals with particular knowledge. A number of individuals were interviewed and in camera hearings were held.
The following key statistics underpin the operations of the Commission:

- 105 requests for written information were issued
- 43 requests for the provision of documents were issued
- nine summonses for attendance at a hearing were issued
- 25 requests for attendance to be interviewed were issued
- six in camera hearing days were held
- 75 submissions were received.

1.4 The 2013 legislation

In June 2015, in accordance with its election commitment, the Queensland Government established the Queensland Taskforce on Organised Crime Legislation (the Taskforce). Pursuant to its Terms of Reference, the Taskforce is required to recommend how best to repeal, or replace by substantial amendment, the 2013 legislation.

The Taskforce is chaired by Mr Alan Wilson, former justice of the Supreme Court of Queensland. Membership of the Taskforce consists of senior representatives from the Department of Justice and Attorney-General, the QPS, the Department of the Premier and Cabinet, the Queensland Police Union, the Queensland Police Commissioned Officers’ Union, the Queensland Law Society, the Bar Association of Queensland and the Public Interest Monitor.

The Taskforce’s Terms of Reference require the Taskforce to have regard to the report and recommendations of the Commission, so far as it is relevant to the Taskforce’s review.

There is obvious overlap between the Terms of Reference of the Commission and those of the Taskforce, because the Commission was required to examine and evaluate the adequacy of legislation available to law enforcement, intelligence, and prosecution agencies to effectively address organised criminal activity. However, the legislation within the purview of the Commission extends beyond the provisions within the scope of the Taskforce.

The Commission’s approach was to have regard to the 2013 legislation, but did not examine the laws in terms of their adequacy in combatting organised crime, given the creation of the Taskforce specifically established to review those laws.

However, in examining the adequacy of current legislation to effectively address organised crime, the Commission noted offences in New Zealand, Canada and a number of Australian states, which specifically target a person who participates in a criminal group intending to further the group’s criminal conduct.

The Commission concluded that the utility of enacting such offences in Queensland is questionable. The Commission anticipates that its consideration of a ‘participation’ type offence for Queensland will be of significant interest for the Taskforce, because under its Terms of Reference the Taskforce must develop a new offence of ‘serious organised crime’.

The Commission notes that the initial timeframe for the Taskforce review of 18 December 2015 has been extended until 31 March 2016.
(Endnotes)


4 Explanatory Notes, *Vicious Lawless Association Disestablishment Act 2013*.

5 See Appendix 1.

6 See Appendix 1.

7 See Appendix Y.
2.1 Introduction

The organised crime law and order policy debate in Queensland has focused, at least since 2008–2009, on outlaw motorcycle gangs. When introducing the Criminal Organisation Act 2009 into the Queensland Legislative Assembly in October 2009, the then-Attorney-General, the Honourable Cameron Dick MP, observed that in response to outlaw motorcycle gang violence in southern states, other states and territories around Australia had passed similar legislation. The then-Attorney-General asserted that such legislation was necessary for Queensland, to ensure that we were not seen as a ‘safe haven for criminal organisations’ that may be tempted to move their operations to Queensland.¹

The focus of the Newman Government—and, consequently, the focus of law enforcement—was squarely on outlaw motorcycle gangs from October 2013, following the violent public brawl that took place on 27 September 2013 between members of the Bandidos and a rival club member at Broadbeach. Following the incident, the Newman Government announced its intention to ‘crackdown on criminal gangs’.²

On 15 October 2013, the then-Government introduced a suite of legislation (referred to in this report as ‘the 2013 legislation’) into the Queensland Parliament. It was debated and passed in the early hours of the following morning. The speed with which the legislation was enacted—and the resulting lack of public scrutiny—drew criticism. Furthermore, the laws themselves have attracted significant publicity and controversy.

The 2013 legislation particularly focused on outlaw motorcycle gangs, and created new offences and aggravated offences under the Criminal Code. The legislation also changed bail laws, introduced minimum mandatory penalties, increased powers for law enforcement agencies, and introduced vetting in certain licensed industries. The package of reforms included the enactment of the Vicious Lawless Association Disestablishment Act 2013 (the VLAD Act), which provides a crushing mandatory cumulative sentencing regime for people who participate in the affairs of an association and commit declared offences for the purpose of, or in the course of, that participation.

The 2013 legislation included amendments to the Crime and Corruption Act 2001, which gave the Crime and Corruption Commission (CCC) new functions—including the capacity to hold hearings in support of its intelligence function regarding criminal organisations or their participants.

Subsequently, in 2013–2014, the Queensland Government provided funding of $14.2 million over two years to the Queensland Police Service (QPS) to target outlaw motorcycle gangs.³ The Government further allocated $2.5 million towards
Crimestoppers reward payments in relation to outlaw motorcycle gangs. Extra funding was also granted to the CCC, by way of $6.7 million over four years for a one-off program to complement police efforts against the activities of outlaw motorcycle gangs, predominantly on the Gold Coast and Sunshine Coast.

In response, the CCC focused heavily on the activities of outlaw motorcycle gangs. The QPS established Operation Resolute to oversee all activity to address outlaw motorcycle gangs and serious crime activity across Queensland, through Taskforces Maxima and Takeback. From its inception until its closure in August 2015, Operation Resolute maintained a strength of in excess of 200 officers, plus additional officers engaged at a regional level.

### 2.2 Outlaw motorcycle gang criminal activity

The Australian Crime Commission (ACC) states that most outlaw motorcycle gang chapters do not engage in organised crime as a collective unit, but rather as small numbers of members who criminally conspire with other criminals. However, outlaw motorcycle gang members are able to leverage off the gang to aid their criminal activities. Outlaw motorcycle gang members play a prominent role in Australia’s domestic production of amphetamine-type stimulants, and they are also involved in other illicit drug markets, vehicle rebirthing and firearms trafficking. Some members have become involved in serious frauds, money laundering, extortion, prostitution, property crime, and bribing/corrupting officials.

The ACC is the custodian of the National Criminal Target List, which identifies organised crime risks, including nationally significant organised criminal syndicates and individuals impacting on Australia. The Commission is aware that a number of members of outlaw motorcycle gangs are on this list. The ACC has maintained confidentiality over both the number of people on that list and on the numbers who are members of outlaw motorcycle gangs.

The CCC further advised that outlaw motorcycle gangs are the most visible organised crime group involved in the use of violence and extortion in Queensland. Violence is used to extort money and assets from legitimate business owners, non-affiliated drug dealers, rival gangs and people operating in gang territory. The outlaw motorcycle gang brand is heavily relied upon as a means to gain compliance for extortion demands.

The CCC has advised this Commission that outlaw motorcycle gangs play a major role in illicit drug markets in Queensland, and are also involved in other criminal activity. Intelligence suggests that the domestic and international connections of outlaw motorcycle gangs are increasingly exploited, with gangs cooperating with other club chapters as well as with sophisticated and high-threat organised crime groups operating in Australia and around the world.

Under the Newman Government, legislation—which may be described as extreme—was enacted to target outlaw motorcycle gangs. With specific extra funding, the QPS and the CCC focused heavily on the activities of outlaw motorcycle gangs and their members and associates.

However, according to the CCC, the heavy focus on outlaw motorcycle gangs has meant that:

> [the Crime and Corruption Commission] has lost visibility of other areas of organised crime active in Queensland, who are likely to have benefited from and or exploited the opportunity to stay under the law enforcement radar.

Further, the QPS acknowledges that:

> [While] OMCGs [outlaw motorcycle gangs] are an important focus for policing strategies, they are but one of the many types of activities that make the organised crime environment in Queensland.

Another activity is that of fraud. The acting head of the Fraud and Cyber Crime Group within the QPS, Detective Acting Superintendent Terry Lawrence, estimates that there are 320,000 fraud victims within Queensland that the QPS does not have capacity to provide an investigative response to.

This seemingly blinkered focus on outlaw motorcycle gangs is concerning, particularly given that statistics reveal that outlaw motorcycle gang members account for a very small percentage of relevant criminal activity.
The QPS website advises that reported crimes committed by outlaw motorcycle gangs equate to around 0.6 per cent of all crimes in Queensland. This statistic comes with the caveat that crimes by outlaw motorcycle gangs are under-reported, for fear of retribution or because the victim may themselves be involved in criminal activity.14

The arrest statistics for Operation Resolute—the state-wide operation to address outlaw motorcycle gangs and serious crime activity across Queensland—are revealing. In response to information sought by the Commission, the QPS reported15 that in the period from 1 October 2013 to 30 June 2015, outlaw motorcycle gang members were charged with one or more offences on 696 occasions. During that same period, the total number of occasions that persons were charged with criminal offences across the state was 133,883.

Therefore, in the 21-month period of intense law enforcement focus on outlaw motorcycle gangs, members of such gangs only accounted for 0.52 per cent of persons charged with criminal offences throughout Queensland.

The Commission notes that the total number of arrests made by Operation Resolute during the 21 month period was 2236. The higher arrest figure includes not only arrests of members of outlaw motorcycle gangs but also arrests of ‘associates’ of such gangs. Using the higher figure, members of outlaw motorcycle gangs and their associates accounted for 1.7 per cent of criminal activity throughout Queensland for that period.

The Commission has been advised that the 696 occasions that outlaw motorcycle gang members were charged with offences relates to 478 individual persons16 and 1,093 charges. The following provides a breakdown of some of the offences:

- 298 offences (27 per cent) drug-related under the Drugs Misuse Act 1986, of which 199 were related to the possession of dangerous drugs or relevant substances
- 122 (11 per cent) violence-to-persons-related offences (including the offence of extortion) under the Criminal Code
- 55 weapons-related offences under the Weapons Act 1990
- 22 offences related to the unlawful possession of explosives under the Explosives Act 1999
- 208 offences (19 per cent) traffic offences or driving-related offences under Transport and other legislation
- 51 offences under the Bail Act 1980
- 33 offences of assaulting or obstructing police, and 16 offences relating to disobeying a direction or requirement under the Police Powers and Responsibilities Act 2000
- 30 public-nuisance-type offences under the Summary Offences Act 2005
- 27 offences related to conduct at licensed premises under the Liquor Act 1992

The Commission notes that, of the 1,093 offences that outlaw motorcycle gang members were charged with, 52 per cent of these (572 offences) are simple offences. A simple offence is one that must be dealt with in a Magistrates Court, and not on indictment in the higher courts. Offences categorised as simple offences are less-serious offences, which carry lesser maximum penalties. Serious offences are indictable offences that must be dealt with in the higher courts upon indictment—unless, under the relevant statutes, they can be dealt with summarily. Indictable offences are crimes and misdemeanours that carry significant periods of imprisonment by way of maximum penalties.

Of the 1,093 charges, 605 have been finalised by way of pleading guilty or of a finding of guilt, and 94 charges were finalised by way of acquittal or of the prosecution offering no evidence. The remainder are yet to be finalised and are before the courts.

The Commission accepts the involvement of outlaw motorcycle gangs in organised crime.

However, in the period of October 2013 to 30 June 2015, a period of intense law enforcement focus on outlaw motorcycle gangs and their members and associates, members of such gangs only accounted for 0.52 per cent of persons charged with criminal offences throughout Queensland.
The Commission shares the concern held by the CCC that the intense focus on outlaw motorcycle gangs has left a hole in the knowledge held by law enforcement in regards to other forms of organised crime networks. Indeed, the evidence before the Commission suggests that the focus upon—and resources solely dedicated to—the threat of outlaw motorcycle gangs has meant that other types of organised crime have not been able to be appropriately investigated. This view is outlined in the chapter on financial crimes.

**Recommendation**

The Commission recommends that:

2.1 The Crime and Corruption Commission extend the focus of its intelligence and research functions beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland.

2.2 The Queensland Police Service extend the focus of its policing strategies beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland.

(Endnotes)


2 Explanatory Notes, *Vicious Lawless Association Disestablishment Act 2013 (Qld)*.


7 Statutory Declaration of Ross Barnett, 2 September 2015.


12 Submission of Queensland Police Service, 22 May 2015, p. 4.

13 Statutory declaration of Terry Lawrence, 28 August 2015, para 18.


3.1 Introduction

In accordance with its Terms of Reference, the Commission inquired into the extent, nature, and economic and societal impacts of organised crime in Queensland in respect of the illicit drug and precursor markets. In particular, the Commission has examined methylamphetamine, cocaine, heroin, 3,4-Methylenedioxyamphetamine MDMA/‘ecstasy’, cannabis, and drug analogues and new psychoactive substances.

Under Queensland’s Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987, such substances are prohibited, and the unlawful possession, production and supply of, and trafficking in, these drugs is a crime.

It is widely accepted that organised crime is entrenched in the drug market in Australia. As at June 2015, indicative figures drawn from the Queensland Police Service (QPS) intelligence reveals that 76 per cent of identified organised crime networks are involved in the illicit drug market, with 51 per cent linked to methylamphetamine, 30 per cent to cannabis and 12 per cent to MDMA/‘ecstasy’. Over one third of organised crime networks linked to the illicit drug trade are involved with multiple drug types. The increasing flexibility with which organisations move between commodities shows the willingness and capability of networks to meet the dynamic demands of the illicit drug market.1

The Crime and Corruption Commission (CCC) told this Commission that illicit drug markets remain the most prominent and visible form of organised crime activity in Queensland, and spoke about the substantial growth in illicit markets for non-traditional drugs—such as performance and image-enhancing drugs—and new and emerging psychoactive substances.2

This chapter examines the indicia of the dangerous drugs listed above, the drugs’ prevalence, the effects of such drugs on the individual, and the impacts on society. This chapter also considers the extent and nature of the involvement of organised crime in the drug trade, and identifies those drugs that are increasing in their use and production throughout Queensland.

To assist in identifying the prevalence of organised crime in the drug trade, the Commission requested details of the number of indictments presented in Queensland within a stipulated time period relating to trafficking offences, with respect to each of the above drugs and those where three or more people were co-accused. Unfortunately, the Office of the Director of Public Prosecutions (ODPP) was unable to provide such information, because their computer systems did not enable them to undertake such a search.3 However, the CCC was able to assist this Commission with information and intelligence.
This chapter considers the legislation and resources available to law enforcement, criminal intelligence, and prosecution agencies in Queensland to prevent and effectively investigate and prosecute organised criminal activity. The Commission is of the view that extensive search, seizure, and covert investigative powers are available to Queensland police when investigating drug offences. However, the Commission recommends amendments to the Drugs Misuse Act and the Drugs Misuse Regulation to provide for a readily transparent and discernable penalty regime, which may have a greater deterrent effect. The Commission has also identified a possible legislative gap: the absence of regulation around the sale and purchase of hydroponic equipment.

The Terms of Reference required the Commission to examine the extent to which those involved in organised crime use—or provide the services of—activities that enable or facilitate organised crime in Queensland. Cyber and technology-enabled crime, pharmacists, violence and extortion, and lawyers were identified as being particularly relevant.

Cyber and technology-enabled crime is increasingly relevant for the drug industry in Queensland, with the Internet and the Darknet enabling the rapid expansion of the global market. The Darkweb is an umbrella term that refers to the anonymous, hidden parts of the Internet not accessible by standard web browsers. Darknet, on the other hand, refers to individual networks within the Darkweb, such as Tor’s Hidden Services, I2P or Freenet. The Surface Web refers to the Internet as the common user would know it, including websites such as Facebook, YouTube and Google.

Individuals based in Queensland can now use Darknets to engage directly with international drug markets and purchase illicit drugs from anywhere in the world, using marketplaces and websites operating on the Darknet and on the Surface Web. This has meant that trends in drug use observed in Europe, Canada and the United States of America, which once would have taken some time to flow on to the Australian market, are now very quickly replicated in Australia.

The Commission notes that the Internet—and particularly the Darknet—creates a low-risk environment for individuals and organised crime groups to purchase and sell dangerous drugs. The anonymity offered by encryption-based services, and supplying via the post, provides protection for offenders. The Commission acknowledges the strong penalties provided in Queensland’s Drugs Misuse Act for the unlawful possession of or supplying in dangerous drugs; however, it is of the view that the Act should be amended to apply increased maximum penalties when such conduct is facilitated by the Internet and Darknet marketplaces.

Organised crime is often supported by—or outsourced to—a range of people with specialist skills or who have access to information or infrastructure. Such ‘facilitators’ may knowingly or unwittingly assist organised crime groups. Criminal groups may target professional facilitators when the group does not have sufficient expertise to carry out a task required to further the unlawful purpose. Criminal groups may also involve such facilitators in an attempt to inject a sense of legitimacy into the criminal enterprise.

For the purpose of examining the illicit drug market, the Commission focused on the roles that pharmacists and lawyers may play as facilitators.

The role of pharmacists is particularly relevant in relation to criminals sourcing pseudoephedrine, the most commonly used ingredient in the making of methamphetamine. Pharmacists are highly regulated. While most comply with their legislative requirements, poor dispensing practices and—in some cases, deliberate unlawful conduct—creates opportunities for criminals. The Commission learned that Project STOP, an online tool that pharmacists can choose to use which tracks pseudoephedrine sales in real time, has had a significant impact on the ability of criminals to source the precursor drug from pharmacies. The Commission understands that 85 per cent of Queensland pharmacies use Project STOP, and that costs associated with the online tool are minimal. This chapter explores Project STOP in detail, with the Commission concluding that its use should be made mandatory by all pharmacies dispensing pseudoephedrine.

With respect to lawyers, the Commission formed the view based on the information before it, that there is no evidence that either solicitors or barristers in Queensland have played a role in facilitating organised crime in the illicit drug market.
The Terms of Reference required the Commission to inquire as to the adequacy and appropriateness of the current responses of Queensland law enforcement, intelligence, and prosecution agencies to prevent and combat organised crime in Queensland. Further, the Commission was to examine the adequacy of cross-jurisdictional arrangements, including the effective co-operation of Queensland law enforcement agencies with Commonwealth law enforcement agencies.

The chapter examines the current procedures in place with respect to the QPS, the CCC, and the ODPP, and highlights good practice and identifies inadequacies.

(Endnotes)

1 Statutory Declaration of Ross Barnett, 18 June 2015, para 6 [In - Confidence]; Submission of Queensland Police Service, 22 May 2015, p. 5.
3 Letter from Crown Law on behalf of Mr Michael Byrne QC, A/DPP, 3 August 2015 [In-Confidence].
5 Egan, M. (2015). What is the Dark Web? How to access the Dark Web – How to turn out the lights and access the Dark Web (and why you might want to). Available at www.pcadviser.co.uk
8 Submission of Crime and Corruption Commission, 22 May 2015, p. 35.

3.2 High-threat illicit drugs

3.2.1 Methylamphetamine

The drug and its effects on the user

Under Queensland’s Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987, methylamphetamine is a prohibited drug, and the unlawful possession, production and supply of, and trafficking in, the drug is a crime.

Methylamphetamine is an addictive central nervous system stimulant, which speeds up the messages travelling between the body and the brain.¹ Methylamphetamine is known to produce intense feelings of pleasure, and can increase a person’s mood, alertness and physical activity while decreasing one’s appetite.² In addition, methylamphetamine is relatively easy to use, readily available, and provides a more sustained and intense feeling of pleasure than other illicit drugs.³ These are all factors that have led to the popularity of this illicit drug.⁴

Methylamphetamine, also sometimes called ‘methamphetamine’, can come in a number of different forms. It commonly presents as crystal (‘ice’), base (‘paste’) and powder (‘speed’), but it may also come as a tablet and, less commonly, as a liquid.⁵ Within Australia, the most common forms of methylamphetamine are ice and speed.⁶

Crystal methylamphetamine is often referred to as ice because it appears as crystals or as a crystalline powder.⁷ Ice is a more purified form of methylamphetamine than speed,⁸ although it can be mixed or ‘cut’ with other substances, which decreases its purity and increases the weight sold.

Ice can be ingested in a number of ways. It is usually smoked by heating the crystals and inhaling the vapours in a glass pipe, but it can also be injected.⁹ Some users also swallow or inhale (‘snort’) the drug.¹⁰ Ice (crystal methylamphetamine) is also known as ‘crystal meth’, ‘batu’, ‘crystal’, ‘d-meth’, ‘glass’, ‘meth’, ‘shau’ and ‘tina’.¹¹
Ice is generally stronger and more addictive than powdered methylamphetamine, and it also has more harmful side effects.12

Powdered methylamphetamine—or speed—is usually white, yellow or brown with a distinctive smell.13 It can be inhaled or snorted through the nose, swallowed, or injected.14 It may also be referred to as ‘crank’, ‘fast’, ‘goey’, ‘loewe’, ‘lou reed’, ‘P’, ‘pep pills’, ‘meth’, ‘rabbit’, ‘tail’, ‘uppers’ and ‘whiz’.15

The base or paste may come as a damp powder,16 or it may appear as an oily or sticky paste.17 Those taking the base or paste form of speed may swallow, snort, or inject the drug.18 It may be referred to as ‘base meth’, ‘pure’ or ‘wax’.19

Methylamphetamine in tablet form is typically swallowed.20 It is often pressed into a tablet with other substances and sold as MDMA or ‘ecstasy’, or promoted as an ‘ecstasy’ alternative.21 In a liquid form, it has a red/brown colour22 and may be injected or swallowed.23 Liquid methylamphetamine may be known among users and suppliers as ‘leopard’s blood’, ‘oxblood’, ‘liquid red’ and ‘red speed’.24

Methylamphetamine appeared in Australia in the late 1990s. Prior to this, the related drug ‘amphetamine’ was available and commonly marketed as speed.25 These days, the drug sold as speed is usually made from methylamphetamine, not amphetamine.26 Methylamphetamine has a stronger effect on the user than amphetamine,27 but both substances belong to the same group or family of drugs referred to as ‘amphetamine-type stimulants’.

‘Amphetamine-type stimulants’ is the term used to describe drugs that are chemically related to amphetamine.28 The term usually includes amphetamines, methylamphetamine, and drugs known as phenethylamines.29 MDMA/’ecstasy’ is also included in the term ‘amphetamine-type stimulant’,30 as it is classed as a phenethylamine.31 Sometimes the term ‘amphetamines’ is used generally to refer to all drugs that fall within this family.32

Amphetamine-type stimulants are synthetic drugs,33 which means they are not found in nature, but are rather made through mixing and processing chemical ingredients together.34 Although some drugs in the amphetamine family are made legally and are used to treat medical conditions,35 most synthetic drugs on the illicit drug market are produced in illegal clandestine laboratories.36

There are a number of chemicals—often called ‘precursors’—that are used to make methylamphetamine. Although the term ‘precursors’ can be narrowly defined to apply to substances used in a particular part of the drug-making process, in this context, the term ‘precursor’ refers to all substances that can be used to make illicit drugs.37 The key precursors for methylamphetamine are substances known as ‘ephedrine’ and ‘pseudoephedrine’.38 Both of these substances have legitimate medicinal purposes. For example, ephedrine is sometimes used as a cough medicine, and pseudoephedrine is commonly used as a nasal decongestant.39

Other substances that are used in the manufacture of methylamphetamine include:

- pentyl-2-propanone or ‘P-2-P’40
- hydriodic acid
- hypophosphite salts
- hypophosphorous acid
- iodine
- phenylalanine
- phosphorous
- lithium metal.41

The majority of precursors listed above are ‘controlled substances’ for the purpose of the Drugs Misuse Act and Drugs Misuse Regulation. This means that there are restrictions around the supply of these substances under the Drugs Misuse Act, and it is an offence to unlawfully possess (section 9A), supply (section 9B), produce (section 9C) or traffic (section 9D) these substances where they exceed certain weights. It is also an offence to possess certain combinations of items, which may include some of these controlled substances under section 10B of the Drugs Misuse Act. The maximum penalties range from 15 to 25 years imprisonment,
depending on the offence. In Queensland, offences may also attract Commonwealth charges brought under the Commonwealth Criminal Code. An example of a Queenslander being charged with importing controlled substances is found in the case study of R v Chandler below.

**Case study**

**R v Chandler**

In the case of *R v Chandler* [2010] QCA 21, Chandler pleaded guilty to one count of importing a commercial quantity of a controlled drug with the intention that it be used to manufacture a controlled drug.

Two parcels from Thailand containing pseudoephedrine addressed to a post office box in Nambour were intercepted at the Sydney Mail Exchange. The parcels were reconstituted with white power and forwarded to Chandler’s address. A third parcel was received shortly thereafter. Telecommunication evidence confirmed that Chandler was aware that the parcels contained pseudoephedrine and were to be used to produce methamphetamine.

The total pure weight of pseudoephedrine found in the three parcels was between 2.79 kilograms and 2.98 kilograms. It could have been used to produce 2 to 2.2 kilograms of pure methamphetamine with a street value of between $600,000 and $1.6 million.

The Court held that Chandler was motivated by profit and that the offence involved a large commercial amount of precursor substance. Chandler was sentenced to five years imprisonment with a non-parole period of three years. This sentence was not disturbed on appeal.

In Queensland, methylamphetamine and amphetamine are listed as dangerous drugs in Schedule 1 of the Drugs Misuse Regulation. Accordingly, trafficking (section 5), supplying (section 6), producing (section 8) or possessing (section 9) the drug is punishable under the Drugs Misuse Act with a maximum penalty of 15 years to life imprisonment, depending upon the particular circumstances and the weight of the drug involved.

**Effects of methylamphetamine on the user**

Methylamphetamine affects the user by interacting with chemicals in the brain called neurotransmitters. Methylamphetamine affects a number of neurotransmitters, including noradrenaline and serotonin. However, the sense of euphoria from methylamphetamine is usually attributed to how it interacts with a neurotransmitter called dopamine. Dopamine plays a role in rewarding people for engaging in essential human behaviours like eating, drinking and sexual activity. It makes people feel pleasure or euphoria so that they will be motivated to do the action again. Dopamines are also involved in controlling movement, attention and memory.

When people take methylamphetamine, they flood their brain with dopamine, causing intense feelings of wellbeing. Methylamphetamine not only causes an increase in the release of dopamine in the brain, but it also stops the chemical from being cleared from the brain, which means that the dopamine levels remain high for a longer period of time than they would when released normally. This also means that once the effects of the drug begin to wear off, the brain may have depleted its dopamine stores, so that there are too few dopamines present, and a person may feel particularly low.

Although cocaine has a similar effect on the brain, methylamphetamine has longer-lasting effects than cocaine. Animal studies have also indicated that methylamphetamine leads to higher levels of dopamine in the brain.
Methamphetamine also causes an increase in the chemical noradrenaline in the brain. Noradrenaline plays a role in preparing a person to either run away from a threatening situation, or to stand and fight against a perceived threat. This is commonly known as the ‘fight or flight’ response. Some have suggested that the effect of methamphetamine on noradrenaline may increase the risk of a person on the drug becoming aggressive or violent.

The euphoric or ‘high’ feelings from methamphetamine may last from seven to 24 hours, or even longer. The length and intensity of the high depends on how a person uses it. Those who inject or smoke the drug feel the effects more quickly and intensely than do those snorting the drug. A person who swallows the drug will feel less intense sensations than when snorting, and it will take even longer for them to feel the effects.

The use of methamphetamine in all its forms can pose serious health risks to the user. These effects may be temporary and short-lasting, or they may lead to serious long-term health complications and even death.

**Short-term effects of methamphetamine**

In addition to the feelings of euphoria, alertness and energy, there are a number of other short-term effects of methamphetamine use, many of which may be unwanted or negative. These include an increased heart rate, faster breathing, jaw clenching, teeth grinding, repetitive behaviour like scratching and itching, sweaty or clammy skin, increased body temperature, loss of appetite, difficulty sleeping, a dry mouth, looking pale, headaches, feeling dizzy, shaking, increased risk taking, restlessness, irritability, aggressiveness, paranoia and, in some instances, psychosis. Due to the high purity of the crystalline form of methamphetamine, these effects are likely to be worse for ice users than for users of speed and base methamphetamine.

**Methamphetamine-related fatalities**

Methamphetamine use has, in some instances, resulted in the deaths of users. The National Drug and Alcohol Research Centre, in a national review of accidental deaths caused by methamphetamines (either by intentional use or by accidental poisoning), found that between 1997 and 2011, methamphetamines were the underlying cause of death of approximately 239 people between the ages of 15 and 54 years. Additionally, a further 1,080 deaths occurred in that period for persons in the same age group where methamphetamine was noted as present, but not primarily responsible for those deaths.

Projected estimates for 2012 and 2013 show increasing trends in both methamphetamine deaths and in deaths where methamphetamine is noted; however, these projections are subject to change and revision.

**Methamphetamine-induced psychosis**

The Australian Medical Association has raised particular concerns regarding methamphetamine-induced psychosis. Such psychosis usually lasts between two to three hours, and can occur both in people with vulnerabilities and in those who are ordinarily ‘psychologically robust’.

The increased risk of psychosis while under the influence of methamphetamine is supported by a study of methamphetamine abusers that found that the risk of experiencing psychotic symptoms when using methamphetamine rose from seven per cent during periods of abstinence to 48 per cent when heavily using methamphetamine. When combined with alcohol and/or cannabis use, that figure rose again to between 61 and 69 per cent. Similarly, an Australian study recently concluded that those who use crystal methamphetamine were five times more likely to suffer psychotic symptoms while using the drug than when they were abstinent.

**Violence and methamphetamine use**

One of the most commonly reported side effects of methamphetamine use is an increased propensity for aggression and violence. There is limited data available on the occurrence of violence while under the influence of methamphetamine. However, a 2008 study of methamphetamine and opioid users found that methamphetamine use was a significant predictor of recent violent offending among participants. In particular, the study found that frequent use of methamphetamines was indicative of higher levels of violent offending.
In that study, those who used methylamphetamines and opioids were twice as likely to have committed a violent offence in the month preceding the study than those only using opioids.\textsuperscript{72} The study also found that those using methylamphetamine were more likely to have been charged with assault and weapons offences in the preceding twelve months.\textsuperscript{73} However, other factors such as drug dealing, problematic alcohol use, conduct disorder and youth all increased the risk of committing violent crimes.\textsuperscript{74}

It should also be noted that the majority of participants in the study—including users of opioids, methylamphetamine, and both drugs in combination—had been the victims of violent crime.\textsuperscript{75}

Results of a study conducted in 2009–2010 on drug use among police detainees found ‘amphetamines’ present in 13 per cent of alleged violent offenders. ‘Amphetamines’, for the purpose of the study, included methylamphetamine, MDMA, and other amphetamines, although the majority tested positive for methylamphetamine.\textsuperscript{76} The class of drugs defined by the study as ‘amphetamines’ was the fourth-most commonly detected drug among violent offenders behind cannabis, benzodiazepines (tranquilisers) and opiates (drugs from the opioid family including heroin).\textsuperscript{77} However, in 2012, the prevalence of methylamphetamine among alleged violent offenders increased to 21 per cent, and that drug was more commonly present among these offenders than benzodiazepines.\textsuperscript{78}

It has been suggested that violence among those who use methylamphetamine may be influenced by a number of factors including predisposition to violence, contextual factors such as involvement in the illicit drug market, and the effects that the drug has on the person using it.\textsuperscript{79}

An explanation for why methylamphetamine use is associated with violence may be that when a person uses methylamphetamine heavily, the parts of the brain involved in controlling emotions are affected, which can increase aggression.\textsuperscript{80} In addition, when using the drug, the release of the chemical noradrenaline can produce a ‘fight or flight’ response in a user, which in threatening circumstances may lead to violent behaviour.\textsuperscript{81}

The potential relationship between methylamphetamine use and violence is not only a concern for those using the drugs, but for the wider community. In particular, it may increase the risks that a methylamphetamine user’s family and friends—and those who may come into contact with the user while they are on the drug, such as health workers and law enforcement officers—will be subjected to violence.

**Coming off the drug**

In the days following methylamphetamine use, people may experience a number of adverse effects known as ‘come down’ effects. Some of these effects include exhaustion, difficulty sleeping or increased need for sleep, decreased appetite, irritability, feeling down or depressed, headaches, dizziness, blurred vision, paranoia, hallucinations and confusion.\textsuperscript{82} The effects of ‘coming down’ may be more severe following the use of ice.\textsuperscript{83}

**Long-term effects**

Some of the concerning long-term effects of methylamphetamine use include decreased memory and concentration, weight loss, malnutrition, exhaustion, irritability and agitation, mental health problems including anxiety, depression and psychosis, dependency on the drug, and a compromised immune system that can lead to regular bouts of sickness.\textsuperscript{84} Users of ice may be particularly susceptible to suffering from more agitation and a higher likelihood of addiction than users of other forms of the drug.\textsuperscript{85}

In some circumstances, the use of methylamphetamines—particularly heavy and regular use—may also cause or contribute to dental issues, to kidney problems including kidney failure, and to heart conditions or a heart attack, and may also increase the risk of a stroke.\textsuperscript{86}

As methylamphetamines can increase risk-taking behaviour and sex drive, it may also lead to unplanned pregnancies and sexually transmitted diseases.\textsuperscript{87}
Neurological effects

There are also a number of neurological effects that methylamphetamine abuse can have on a person, with some studies on chronic methylamphetamine users showing changes in the structure and functioning of the areas of the brain involved in emotion and memory. These changes may account for the emotional and cognitive issues suffered by some methylamphetamine users.

Dependency

One of the greatest risks to the health and wellbeing of an individual taking methylamphetamine is the risk of dependency. Although all forms of methylamphetamine may result in addiction by the user, those who use crystal methylamphetamine—or ice—are particularly vulnerable to developing a dependency on the drug. Abuse of methylamphetamine and other amphetamines occurs when someone continues to use the drugs despite negative impacts and consequences on their life. When a person becomes dependent on a drug, that abuse is usually accompanied by tolerance to the drug, withdrawal symptoms when a person is not able to use the drug, and compulsive behaviour.

Some of the symptoms of withdrawal from ice and other forms of methylamphetamines and amphetamines include cravings, mood swings (including feeling irritable, stressed, agitated, restless, anxious, bored, easily upset and depressed), feeling tired and run down, having difficulty concentrating, aches and pains, restless sleep, headaches, increased appetite, nightmares, depression and paranoia. Some of these symptoms may only last a few days or weeks, and others may last for a month or more.

Those who become dependent upon and tolerant to methylamphetamines are likely to use higher doses more regularly. This increases the risks of suffering adverse health effects from such drug use. It also increases the likelihood that the user will have financial, employment, legal and other social issues arising from their dependency.

Health risks associated with polydrug use involving methylamphetamine

Another factor that increases the risk of suffering adverse health effects for methylamphetamine users is the practise of using the drug in combination with other substances. Many people who use methylamphetamine also use other drugs such as cannabis and MDMA/’ecstasy’. The practise of combining multiple drugs is often referred to as ‘polydrug use’. Methylamphetamine use in conjunction with other substances can increase the risk of negative health and social implications for an individual. Some examples of these consequences include:

- Use of ice together with alcohol, cannabis, or benzodiazepines (tranquillisers) can increase the risk of overdose, because the ice can mask the effects of those other drugs, leading people to overdose.
- Use of alcohol and methylamphetamines together can increase blood pressure, placing greater strain on the heart.
- Use of alcohol and methylamphetamine together may also increase the risk of accidents, because a person using both may have a false sense of sobriety and of being in control.
- Use of methylamphetamine and cannabis together can increase psychotic symptoms in some people.
- Use of heroin and methylamphetamine together can slow down breathing, which can cause heart failure.
- Use of heroin and methylamphetamine together can also increase the risk of a heroin overdose.
- Use of cocaine and methylamphetamine together can increase the negative effects that each drug has on a user’s heart.

In many cases, people use other drugs such as cannabis or tranquillisers to offset the effects of methylamphetamine—for example, to help them sleep. This practice can lead to dependency on multiple different drugs, and can increase the overall risk of having serious physical and psychological problems.
Health risks associated with method of administering methylamphetamines

The way a person chooses to take methylamphetamines may also present distinct health problems to a user. Those who choose to inject methylamphetamines are particularly at risk of contracting a number of serious illnesses if they share or re-use needles or other equipment.

Some of these health consequences include contracting blood-borne viruses such as hepatitis B, hepatitis C and human immunodeficiency virus (HIV).\textsuperscript{105} Hepatitis C is particularly common among injecting drug users in Australia.\textsuperscript{106} Injecting drugs can also lead to serious infections—including infections that can cause heart problems—and it may cause blood clots in veins.\textsuperscript{107} Injecting drug users may also suffer from skin sores or abscesses.\textsuperscript{108}

Those who smoke methylamphetamines are at risk of causing damage to lung tissue, causing bleeding in the lungs or, in some cases, a build-up of fluid in the lungs.\textsuperscript{109} Smoking and injecting methylamphetamines also increases the risk of addiction.\textsuperscript{110}

Snorting methylamphetamines can cause nose bleeds and damage the nasal passages.\textsuperscript{111}

There are a number of serious consequences to an individual from methylamphetamine use, many of which are particularly pronounced for those who use the drug in the crystalline or ice form. Given the prevalence of the drug in the community, and given the increasing use of ice as the most commonly used form of methylamphetamine, this poses a great risk to the community.

Costs of health care related to methylamphetamine

The negative health effects of methylamphetamine use also impact the community through the provision of health care services to users.

In 2012–2013, amphetamines (not including MDMA/’ecstasy’) were the principle drug of concern in 3,215 closed treatment episodes for drug use in Queensland.\textsuperscript{112} A closed treatment episode refers to a period of contact between a client and a treatment agency or service that has defined dates for the commencement of the treatment and the cessation of treatment.\textsuperscript{113} Behind cannabis, amphetamines accounted for the second-most closed treatment episodes out of the illicit drugs.\textsuperscript{114} Amphetamines accounted for 10.9 per cent of closed alcohol and drug treatment episodes, with treatment for alcohol and cannabis being the only other substances accounting for a greater per cent of treatment episodes.\textsuperscript{115}

Nationally, there were 22,265 closed treatment episodes for drug use where amphetamines were the principle drug of concern, with cannabis the only other illicit drug accounting for more treatment episodes.\textsuperscript{116}

In Queensland, the estimated spending for 2012–2013 on alcohol and other drug services was $226,977,266, which is approximately 19.2 per cent of the national expenditure on alcohol and other drug treatment.\textsuperscript{117} Having regard to the proportion of treatment episodes where amphetamines are the principle drug of concern in Queensland, this treatment cost approximately $24,833,491. This figure is a general estimate and should be treated with caution as the costs allocated to specific types of treatments sought by amphetamine users have not been considered.

These do not include figures for treatment of illnesses such as heart or kidney disease or hepatitis that may be related to a person’s use of methylamphetamine, and only give a small indication of the costs to the health care system caused by amphetamine-type stimulants.

The prevalence of methylamphetamine

The prevalence of methylamphetamine around the world

In 2013, it was estimated that approximately 246 million people worldwide between the ages of 15 and 64 years—or around 5.2 per cent of the global population—had used an illicit drug at least once in the previous year.\textsuperscript{118} Amphetamine-type stimulants and prescription stimulants, excluding MDMA/’ecstasy’, were
considered to be the second-most commonly used drugs in the world behind cannabis, with between 13.9 million and 53.8 million people estimated to use these kinds of drugs that year.

The best annual estimate from the United Nations Office on Drugs and Crime (UNODC) was that, in 2013, approximately 33.9 million—or around 0.7 per cent of the population—used amphetamine-type stimulants and prescription stimulants.

Oceania (with data primarily from Australia and New Zealand) is the region with the highest estimated use of amphetamine-type stimulants worldwide, with approximately 2.1 per cent of the population using the drug in 2013. Use above the global average is also found in the Americas, with particularly high use in the Caribbean and in Central and North America. Africa also has use above the global average.

Use of amphetamine-type stimulants appears to have remained relatively stable in recent years, with a small decrease in global prevalence in 2013. Despite this, there are also a number of areas that have a growing methylamphetamine market. In 2012, there was evidence of emerging markets in Central Asia, Transcaucasia (a region located on the border of Eastern Europe and Southwest Asia), and Pakistan. There were also indications in 2012 of increasing use in East and South-East Asia. In 2013, there were indications of increasing use of methylamphetamine in North America and Europe.

Although use of the group of substances globally has remained relatively stable in recent years, seizures of amphetamine-type stimulants—particularly methylamphetamine—increased in 2012 before decreasing moderately in 2013. In 2012, global seizures of amphetamine-type stimulants reached a record high of 144 tons, which was a 15 per cent increase from 2011. Approximately 80 per cent of those seizures were for methylamphetamine, which accounted for 114 of the 144 seized tons. According to UNODC, global seizures of methylamphetamine have almost quadrupled since 2008. This is evidenced by the table below, which shows the global seizures of amphetamine-type stimulants in the years from 2003–2012, with methylamphetamine, amphetamine, and ecstasy-type substances highlighted.

![Global seizures of amphetamine-type stimulants, 2003-2012](image)

The majority of methylamphetamine seizures in 2012 were in North America, which accounted for nearly two-thirds of the seizures. This was followed by East and South-East Asia, which accounted for one-third of seizures.

In 2013, seizures decreased slightly, with approximately 124.2 tons of amphetamine-type stimulants—including ‘ecstasy’—seized. Although lower than the seizures in 2012, when reviewed against the table of 2003–2012 seizures above, the figures are similar to those recorded in 2011, and seizures in 2013 were still higher than any seizures in the 2003–2010 period. In 2013, 88 tons of the amphetamine-type stimulants seized were made up of methylamphetamine.
Between 2011 and 2012, the number of detected laboratories producing amphetamine-type stimulants increased from 12,571 to 14,322. Of these laboratories, 96 per cent were making methamphetamine. The number of methamphetamine laboratory detections particularly increased in the United States and Mexico in 2012. According to the Australian Crime Commission (ACC), crime groups in China, Burma, Indonesia, Mexico and Iran are some of the largest global producers of methamphetamine, with the Philippines, Russia and Ghana also emerging as production hubs for the drug.

In Europe, amphetamine is more commonly used than methamphetamine, although the European Monitoring Centre for Drugs and Drug Addiction has recently received reports that the availability of methamphetamine is increasing.

Global seizures and laboratory detections indicate that methamphetamine is becoming the most common form of amphetamine-type stimulant on the global market. Despite generally low use in Europe, methamphetamine is popular in Oceania, the Caribbean, and Central and North America. Despite a recent decrease in global prevalence of amphetamine-type stimulants and prescription stimulants, drugs from the amphetamine-type stimulant family remain the second-most prevalent type of illicit drug in the world, indicating that there is a high global demand for methamphetamine. This provides opportunities for transnational organised crime groups to remain prominently involved in trafficking methamphetamine and precursor chemicals around the world.

The prevalence of methamphetamine in Australia

Around eight million Australians aged 14 years or over—or 42 per cent of the population—have reported using an illicit drug in their life, with 2.9 million Australians—or approximately 15 per cent of the population—using an illicit drug in the year preceding the 2013 National Drug Strategy Household Survey (‘survey’). According to the most recent survey, in 2013 approximately 1.3 million Australians—or seven per cent of the population—had tried what the survey refers to as ‘meth/amphetamines’ in their lifetime. It should be noted that prior to 2007, the surveys referred only to ‘amphetamines’, with the term ‘meth’ added in more recent years to reflect the changing use pattern in this market.

In the year preceding the survey, 400,000 people aged 14 years or older—or 2.1 per cent of the Australian population—had used what the survey referred to as ‘meth/amphetamine’. This makes these drugs the third-most popular of the main illicit drugs used in Australia (excluding misused pharmaceuticals), along with cocaine but behind cannabis and MDMA/‘ecstasy’. Despite ‘meth/amphetamine’ being only the third-most commonly used drug in Australia, the ACC has identified methamphetamine as posing the highest risk to the Australian community.

Despite the relative popularity of ‘meth/amphetamine’, its use has been decreasing since a peak in 1998—although its use between 2010 and 2013 did remain stable. Importantly, however, in 2013 the use of ice as the main form of ‘meth/amphetamine’ significantly increased from use by 21.7 per cent of recent users in 2010 to use by 50.4 per cent of recent users in 2013. This is an extremely significant increase, which should be of great concern.

Use of ‘meth/amphetamine’ in powder form has significantly decreased from being the main form of the drug used by 50.6 per cent of recent users in 2010 to being the main form used by only 28.5 per cent of recent users in 2013. Use of base, prescription amphetamines, tablets and liquid also declined in 2013. Australian ‘meth/amphetamine’ users were almost twice as likely to live in remote or very remote areas than they were to live in major cities in 2013. While the use of ‘meth/amphetamines’ in major cities and inner regional areas is less common than it was in 2007, its use in outer regional, remote and very remote areas has increased, when compared with rates of recent use in 2007. This is concerning, because regular use of methamphetamine can lead to a number of adverse health outcomes and dependency. Additionally, those living in remote or very remote areas may have less access to resources, drug treatment programs, and health and mental health facilities to assist them in adequately dealing with the consequences of methamphetamine use.
Those of an average socio-economic status were most likely to use ‘meth/amphetamine’, while people from the most advantaged and second-most advantaged socio-economic groups were the least likely to use the drugs in the 12 months prior to the survey. Those who were unemployed or looking for work were more than twice as likely to take ‘meth/amphetamines’ than those who were employed in 2013.

‘Meth/amphetamine’ users were also more likely to be male than female, and those who were single without children, or single with dependent children, had higher usage rates than people who were in a couple. Use among single people with or without children increased significantly between 2010 and 2013. People who are homosexual or bisexual were 4.5 times more likely to use ‘meth/amphetamines’ than those that were heterosexual in 2013.

Indigenous Australians were 1.6 times more likely to use ‘meth/amphetamine’ than non-Indigenous people in 2013.

Recent ‘meth/amphetamine’ users were also most likely to be between 20 and 29 years of age. However, there has been a general trend of increasing age in Australian ‘meth/amphetamines’ users since 2001, although the median age of users between 2010 and 2013 remained stable.
The age at which people in the age group of 14 to 24 years first tried 'meth/amphetamines' also increased, from an average age of 17.9 years in 2010, to 18.6 years in 2013. A 1995 review of the average age of initiation among people aged 14–24 years supports the fact that the age of first use has increased since that time, with the highest age of initiation (18.6 years) being found in the most recent survey of 2013. Given the negative health impacts that methylamphetamines and amphetamines can have on a user, it is a positive change that users in the 14-24 year age group are waiting longer to first try 'meth/amphetamines'.

On the other hand, there are a number of concerning trends surrounding the use of methylamphetamine. There has been an increase in the proportion of users consuming 'meth/amphetamine' at least once a week or more, increasing from 9.3 per cent in 2010 to 15.5 per cent in 2013. For those consuming ice, the proportion of those using at least once a week or more has more than doubled, from 12.4 per cent in 2010 to 25.3 per cent in 2013.

% of recent users of methylamphetamine and amphetamine using at least once a week or more 2007-2013


Between 2007 and 2010, there was a significant drop in those using ice at least once a week or more; however, in 2013, the rate of those using ice once a week or more exceeded the figures for 2007.

According to the Ecstasy and Related Drugs Reporting System, the median national cost for those purchasing the drugs in the six months before the study was $50 per point (or $250 a gram) for speed, $60 per point (or $200 a gram) for base, and $100 per point (or $500 a gram) for ice. Although ice is priced higher than other forms of methylamphetamine, it can be a cheaper option than speed and base, since a smaller amount is required for use.

A point is approximately 0.1 grams. According to the Ecstasy and Related Drugs Reporting System, those who used speed used a median of half a gram in a typical using session which, based on the median national prices, would amount to around $125. Those who used base used a median of two points in a typical session which would amount to $120 based on the median national prices. Those using ice only used one point per typical session, which cost $100 per session based on the median national price.

A similar study on injecting drug users in 2014 found that the median national price paid for speed in the previous six months was $50 a point, while the median price for base was $100 per point and the median price of ice was $500 per point.

Globally, Australians pay some of the highest prices for methylamphetamines. UNODC has reported that a gram of methylamphetamine in China costs approximately USD$80, whereas the same amount in Australia is approximately USD$500. Although the figures upon which this was based are unclear, it appears generally consistent with reports from the 2014 Ecstasy and Related Drugs Reporting System. That report indicated that the national median price paid for a gram of ice by participants was $500, but ranged up to a median...
of $850 a gram in the Northern Territory.\textsuperscript{179} Therefore, the premium prices paid in Australia make importing methylamphetamine and its precursors into the country attractive to organised crime groups.\textsuperscript{180}

Also concerning is the fact that the purity of methylamphetamine in Australia has apparently been increasing, making the drug even more dangerous.\textsuperscript{181} A review of the \textit{Illicit Drug Data Reports} published by the ACC for the 2009–2010 financial year through to the 2013–2014 year supports an increasing trend in the purity of methylamphetamine, despite being somewhat incomplete.\textsuperscript{182} The table below shows, from available data, the difference in purity between drugs seized by state police in 2009–2010 and those seized by state police in 2013–2014.\textsuperscript{183} In 2013–2014, the median level of purity for each state was the highest on record, with an average increase in purity of 7.4 per cent from the 2012–2013 period to the 2013–2014 period.\textsuperscript{184}

**Median total % purity of methylamphetamine seized by state police 2009-10 compared with 2012-13 (No data for NT or ACT available for state police seizures).**

<table>
<thead>
<tr>
<th></th>
<th>2009-2010</th>
<th>2013-2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasmania</td>
<td>0.00%</td>
<td>20.00%</td>
</tr>
<tr>
<td>Western Australia</td>
<td>40.00%</td>
<td>60.00%</td>
</tr>
<tr>
<td>South Australia</td>
<td>80.00%</td>
<td>80.00%</td>
</tr>
<tr>
<td>Queensland</td>
<td>86.4%</td>
<td>86.4%</td>
</tr>
<tr>
<td>Victoria</td>
<td>73.9%</td>
<td>73.9%</td>
</tr>
<tr>
<td>New South Wales</td>
<td>99.9%</td>
<td>99.9%</td>
</tr>
<tr>
<td>South Australia</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>


Another concerning trend is the increase in the availability and accessibility of ‘meth/amphetamines’ in Australia. According to the National Drug Strategy Household Survey, the percentage of respondents who indicated in 2010 that they had been offered, or had an opportunity to use, ‘meth/amphetamines’ was 3.9 per cent. In 2013, this had increased to 5.8 per cent.\textsuperscript{185} Although the rates were higher in 2004, this is a higher prevalence than in 2007 and in 2010.\textsuperscript{186}

The accessibility of methylamphetamines is also supported by the 2014 Ecstasy and Related Drugs Reporting System, which studied ‘ecstasy’ and other psychostimulant users. Of those responding to a question about the accessibility of methylamphetamines:

- 73 per cent indicated that speed was either ‘easy’ or ‘very easy’ to access
- 72 per cent reported that base methylamphetamine was ‘easy’ or ‘very easy’ to access
- 86 per cent indicated that ice was either ‘easy’ or ‘very easy’ to obtain.\textsuperscript{187}

The prevalence and accessibility of the drug are also reflected in national border interception and seizures of amphetamine-type stimulants. In 2013–2014, the number of amphetamine-type stimulants (excluding MDMA/‘ecstasy’) intercepted at the Australian border increased to the highest on record by 18.04 per cent from 1,999 in 2012–2013 to 2,367 in 2013–2014,\textsuperscript{188} with the previous reporting period also increasing dramatically by 85.6 per cent from 1,077 in 2011–2012 to 1,999 in 2012–2013.\textsuperscript{189}
The total weight of detections decreased from 2,138.5 kilograms in 2012–2013 to 1,812.4 kilograms in 2013–2014. This is, however, the second-highest weight on record, as the total weight of amphetamine-type stimulants (excluding MDMA) was significant in 2012–2013, having increased by 515.8 per cent from the previous year.190

The table below illustrates the rapid rise in detections of amphetamine type substances (excluding MDMA) at the Australian border from 2004–2014.191

Number and weight of ATS (excluding MDMA) detections at the Australian border, 2004–05 to 2013–14 (Source: Australian Customs and Border Protection Service).

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
<th>Weight (kg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-05</td>
<td>500</td>
<td>2500</td>
</tr>
<tr>
<td>2005-06</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>2006-07</td>
<td>1500</td>
<td>1500</td>
</tr>
<tr>
<td>2007-08</td>
<td>2000</td>
<td>1000</td>
</tr>
<tr>
<td>2008-09</td>
<td>2500</td>
<td>500</td>
</tr>
<tr>
<td>2009-10</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>2011-12</td>
<td>1500</td>
<td>1500</td>
</tr>
<tr>
<td>2012-13</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>2013-14</td>
<td>500</td>
<td>2500</td>
</tr>
</tbody>
</table>


The Australian methylamphetamine market has traditionally been supplied by local production.192 Although there has been an increasing trend of methylamphetamines being detected at the Australian border, there does not appear to have been any concurrent fall in domestic production of the drugs,193 which indicates a continuing strong demand.

In 2013–2014, there were 1,035 detections of amphetamine-type stimulant (excluding MDMA) precursors at the border, weighing a total of 1,505.2 kilograms.194 This is a slight decrease from 1,043 precursor detections weighing 1,700.4 kilograms in 2012–2013.195 China was a key source of precursors in 2013–2014; however, intercepted precursors had been sent from 43 different embarkation points.196

Over the past decade, the number of clandestine laboratories detected in the country have increased by 95.3 per cent.197 In 2013–2014, there were 770 clandestine laboratories detected in Australia, 608 of which were producing methylamphetamines and other amphetamine-type stimulants.198 As with a decrease in precursors, this was also a drop from the number of detections in 2012–2013; however, it was still the third-highest number of detections on record.199

Despite the recent decreases in the number of clandestine methylamphetamine laboratories detected and the weight of the drug seized in 2013–2014, the ACC has noted that there has been a trend over the past five years of significant growth in the importation, manufacture and supply of the drug.200

Arrest figures can also shed some light on how commonly methylamphetamines are used and supplied within Australia. In recent years, the number of arrests of methylamphetamine consumers and suppliers has been generally increasing.

In 2013–2014, there were 26,269 arrests of amphetamine-type stimulant suppliers and consumers.201 Of these arrests, providers of amphetamine-type stimulants accounted for 6,265.202 This compares to five years ago, when in 2009–2010, there was a total of 13,982 arrests for amphetamine-type stimulant
consumers and providers, with 3,921 of those arrests for providers. The number of seizures nationwide for amphetamine-type stimulants increased to the largest number on record, from 21,056 in 2012–2013, to 26,805 in 2013–2014.

These figures clearly show that although use appeared to remain stable between 2010 and 2013, there is a significant amount of amphetamine-type stimulants being supplied to the Australian market. These figures support the findings of the National Drug Strategy Household Survey, the Ecstasy and Related Drugs Reporting System, and the Illicit Drug Reporting System, which found that methylamphetamine are readily available.

In addition to the high national arrest rates for amphetamine-type stimulant offences, 33.0 per cent of tested police detainees returned positive results to methylamphetamines in 2013–2014. This was an increase from 25.9 per cent in 2012–2013, and was the highest rate of methylamphetamine detection in detainees in the past decade. In addition, 48.9 per cent of detainees participating in the Drug Use Monitoring Program reported that they had used methylamphetamines in the 12 months prior to being detained.

Given these trends, it is understandable that the use of ‘meth/amphetamine’ is a concern to the Australian public. In the National Drug Strategy Household Survey in 2013, ‘meth/amphetamines’ were nominated as the illicit drug of most concern to the general community. These types of drug were considered the second-most likely illicit drug, after heroin, to cause the most deaths in Australia.

Although use of ‘meth/amphetamines’ has decreased since 1998 and remained stable more recently, the trend of increased use of ice or crystal methylamphetamine is concerning, because it is more addictive than other forms of methylamphetamine such as speed, and it has more harmful side effects.

It is also alarming to consider the ease with which people can access ‘meth/amphetamine’, the increase in the frequency of use of the drugs, and the higher levels of purity seen in recent years. These changes in the market pose higher risks to the health and wellbeing of individuals using the drugs, and also to the community as a whole, who ultimately have to shoulder the burden of health and social costs.

Given the increasing concern surrounding the prevalence of ice, in 2015 the Federal Government announced that it would be developing a National Ice Action Strategy to deal with the problem of ice as a form of methylamphetamine use around the country. To develop and implement this strategy, a National Ice Taskforce was established. The Taskforce is working with states and territories to:

- examine existing efforts to address ice at all levels of government
- receive submissions from community consultations and expert groups
- identify gaps in knowledge around treatment models, criminal activity and the impact of ice on vulnerable groups—including its impact on people that live in regional areas and Aboriginal and Torres Strait Islanders
- identify initiatives that are having positive outcomes for the community
- find ways to ensure that current efforts to deal with ice are sufficiently targeted, effective and efficient
- advise on prevention activities based on evidence and best practice
- consider options to improve coordination and collaboration of existing local, regional, state and territory efforts
- develop recommendations to be actioned as part of developing a National Ice Action Strategy.

The former Prime Minister presented the National Ice Taskforce interim report to the Council of Australian Government’s meeting on 23 July 2015. On 16 August 2015, the former Prime Minister announced that the Commonwealth Government would make $1 million available to establish a ‘dob-in-a-dealer’ telephone hotline to encourage ‘the community fight against the ice epidemic’. A final report will be provided by the taskforce to the Prime Minister before the end of 2015.

While the Commission agrees with the establishment of this telephone hotline as part of the recommendations from the taskforce, and while the Federal Government has contributed $1 million towards the establishment of
the actual hotline, the Commission does have some concerns as to how information received as a result of this hotline will be able to be actioned by the QPS. The State Drug Squad would appear to be the body where such information would be provided, and it would be expected that this Squad would need to then investigate such information further. It is important that public confidence in such hotlines as these is maintained, and this would need to be done by the QPS investigating these matters quickly and efficiently.

However, the Commission is aware that the State Drug Squad is already using all resources available to it to action the intelligence that it receives. It is a concern of the Commission that this new hotline—and the resultant intelligence provided from it—may not be able to be resourced effectively by the QPS. It is the recommendation of this Commission that the QPS ensure that there are sufficient resources in place to deal with this additional workload. As a consequence of this recommendation, it is also the view of the Commission that the Queensland Government should support any reasonable request by the QPS for additional funding to meet this additional function.

**Recommendation**

3.1 The Commission recommends that the Queensland Police Service ensure that there are sufficient resources in place to deal with the additional workload generated by the Dob-in-a-Dealer telephone hotline, a Federal Government initiative aimed to attack the ice epidemic.

The Commission is aware that the Queensland Attorney-General is being briefed on the progress of this Taskforce through the National Law, Crime and Community Safety Council. The Commission is also aware that the QPS has provided submissions to the Taskforce.

In March 2015, the Chair and Deputy Chair of the Commonwealth Parliamentary Joint Committee on Law Enforcement also announced an inquiry into the importation, manufacture, distribution and use of crystal methylamphetamine. That committee will focus on law enforcement issues, the involvement of organised crime in methylamphetamine-related criminal activities, the nature, prevalence and culture of methamphetamine use in Australia, and strategies to reduce the high demand for methamphetamine in Australia. As of 20 August 2015, that inquiry had received and published 82 submissions on its website.

**The prevalence of methylamphetamine in Queensland**

According to the CCC:

Methamphetamine is the drug that poses the greatest threat to Queenslanders because of its prevalence across the state, its harms and the strong presence of organised crime in this market.

In Queensland, the use of ‘meth/amphetamines’ is above the national average. Approximately 2.3 per cent of the population reporting in 2013 had used the drug in the previous 12 months.
The illicit drug market

Recent use of methylamphetamine and amphetamine by state 2010 and 2013


'Meth/amphetamines' are the third-most commonly used illicit drug in Queensland (excluding pharmaceuticals) behind cannabis and ecstasy, but are more commonly used than cocaine and heroin.223

Like the national trend, ice use has increased in this state. Between 2010 and 2013, use of ice among people who reported recently using ‘meth/amphetamines’ increased from 19.9 per cent to 45.5 per cent.224 In the same period, use of ‘powder’ among recent ‘meth/amphetamine’ users dropped from 41.6 per cent to 21.2 per cent.225

In Queensland, use of the base form of ‘meth/amphetamine’ also appeared to increase among recent users in 2013, while dropping in all other jurisdictions.226 The CCC has also recently reported the emergence of methylamphetamine oil as a commodity traded in Queensland.227

Arrest and seizure figures also demonstrate an increasing prevalence of the drug. In 2013–2014, Queensland had a total of 6,772 arrests for suppliers and consumers of amphetamine-type stimulants.228 This was the second-highest number of consumer and supplier arrests behind Victoria.229 In recent years, the numbers of arrests for suppliers and consumers of amphetamine-type stimulants in Queensland has steadily been increasing.230 In addition to arrests for supply and possession of the drug, the CCC also reports that there have been several violent offences in Queensland linked with the use of ice.231

The number of seizures of amphetamine-type substances within Queensland also increased by 21.7 per cent from 4,172 in 2012–2013 to 5,077 in 2013–2014.232 The weight of these seizures increased significantly by 433.5 per cent from 58,053 grams in 2012–2013 to 309,720 grams in 2013–2014.232 Queensland recorded the third-highest weight for amphetamine-type stimulant seizures in 2013–2014, behind New South Wales and Victoria.234

Queensland had the highest number of detections of clandestine laboratories producing amphetamine-type stimulants in 2013–2014.235 Queensland accounted for 270 of the 608 laboratory detections, or 44.4 per cent.236 This is concerning, not only because it indicates a high demand for the drug, but also because these laboratories are generally detected in residential areas.237 These laboratories pose significant risks to other residents of the property, to neighbours, and to the surrounding community, because the
The illicit drug market can be highly volatile and they pose explosion risks. They also pose risks of contaminating the local environment.

There have been a number of prosecutions in Queensland for the production of methylamphetamine, as evidenced by the two case studies below.

### Case study

**R v Hurst**

In *R v Hurst* [2014] QCA 168, Dean Hurst pleaded guilty to one count of producing and one count of possessing methylamphetamine. Hurst, and co-accused Hollingworth, had been producing methylamphetamine in a clandestine laboratory underneath a set of stairs in Hollingworth’s apartment. Police found ‘cook’ books and various paraphernalia consistent with the production of methylamphetamine.

The Court held that the production of methylamphetamine was done for a commercial purpose. Hurst was sentenced to three years and four months’ imprisonment for the count of producing methylamphetamine, and four months for possessing the drug. The sentences were ordered to be served concurrently and were ultimately not disturbed on appeal. The Court was satisfied that while Hurst was guilty of acts preparatory to production, there was not sufficient evidence that he had actually produced any methylamphetamine; however, the potential to produce large volumes did exist.

### Case study

**R v Budd**

On 18 January 2012, Andrew Stephen Budd (*R v Budd* [2012] QCA 120) pleaded guilty to one count of producing and 28 counts of supplying methylamphetamine, and one count of possessing a thing used for production of a dangerous drug. A man by the name of Grimm was producing methylamphetamine with the assistance of Budd, who supplied cold and flu tablets to extract pseudoephedrine. Grimm, Budd, and a female worked together to obtain the ingredients for methylamphetamine, with Grimm taking on the role as ‘cook’.

The Court held that Budd was involved in the production of methylamphetamine toward the lower end of the scale. He was a drug-addicted person, who was paid with samples for his assistance in producing the drug. The Court sentenced Budd to 18 months imprisonment. The sentence was not disturbed on appeal.

Despite these examples, and the high figures for clandestine laboratory detections reported by the ACC for the 2013–2014 financial year, the CCC has reported to this Commission that there has been a recent decrease in the number of clandestine laboratory detections in Queensland.

In Queensland, as in other parts of Australia, methylamphetamines appear to be relatively easy to access. Of the Queensland participants who responded to the questions about the availability of various forms of methylamphetamine in the Ecstasy and Related Drugs Reporting System, 78 per cent of those who commented about the availability of methylamphetamine powder or speed said that it was ‘easy’ or ‘very easy’ to obtain, and 94 per cent of those commenting on the availability of crystalline methylamphetamine or ice said that it was either ‘easy’ or ‘very easy’ to obtain.
Base methylamphetamine appeared to be less readily available in Queensland, with 43 per cent of those responding to the availability of base indicating that it was ‘easy’ to obtain and 57 per cent indicating it was either ‘difficult’, or ‘very difficult’ to access.242 This was lower than the national perceived availability of base. However, Queensland respondents reported that speed and ice were either ‘easy’ or ‘very easy’ to obtain at higher rates than the national average.243

A study on injecting drug users also found similar results. In relation to the availability of methylamphetamine powder, 79 per cent of those responding to the question said it was either ‘easy’ or ‘very easy’ to obtain, which was lower than those nationally reporting the same.244 Of those commenting on the availability of crystal methylamphetamine, 92 per cent reported that, in Queensland, it was either ‘easy’ or ‘very easy’ to obtain. This was similar to the national response of 91 per cent, although Queensland had much higher rates of respondents reporting that ice was ‘very easy’ to obtain.245 The study found that 80 per cent of Queensland participants reported that base was either ‘easy’ or ‘very easy’ to obtain, which was slightly lower than the 83 per cent who responded the same nationally.246 The difference between the perceived availability of base in Queensland among MDMA/‘ecstasy’ and psychostimulant users and injecting drug users may be related to the differing context of drug use for these two groups.

A concerning trend in Queensland is the practise of injecting methylamphetamine—particularly ice. Although the 2013 National Drug Strategy Household Survey did not consider how ‘meth/amphetamines’ were administered, recent results from the Illicit Drug Reporting System and from the Ecstasy and Related Drugs Reporting System can shed some light on the use patterns of illicit drug users.

The Illicit Drug Reporting System indicated that in 2014, methylamphetamine was the first drug injected by 59 per cent of Queensland injecting drug users, compared with 48 per cent of national participants.247 This was also an increase from 2013, when only 50 per cent reported that methylamphetamine was the first drug they injected.248 Ice or crystal was slightly less popular in Queensland among injecting drug users than it was nationally.249

The Ecstasy and Related Drugs Reporting System indicates that the number of Queensland MDMA/‘ecstasy’ and psychostimulant users participating in the study who had used methylamphetamines in 2014 was 72 per cent, which was slightly higher than 68 per cent of national respondents reporting use.250 Queensland had higher rates of people reporting ‘binging’ (using over 48 hours without sleep)251 on ice, with 44 per cent admitting to the practise in Queensland, compared with 30 per cent reporting binging on ice nationally.252 However, Queensland MDMA/‘ecstasy’ and psychostimulant drug users were less likely to binge on speed than the national average.253

A concerning trend reported in the Ecstasy and Related Drugs Reporting System is the fact that Queensland has higher injecting rates for speed, base and ice than the national averages.254 This is concerning, because injecting drugs puts a person at risk of suffering from additional serious health concerns like infections and viruses, and also because injecting crystal methylamphetamine is the most addictive way to use the drug.255

Although the national rates of ‘meth/amphetamine’ use have been decreasing in recent years—and remained stable between 2010 and 2013—in Queensland, use of the drugs has increased. What is particularly concerning is the increase in popularity of crystal methylamphetamine in the state. If reports from the Ecstasy and Related Drugs Reporting System are accurate, the high rates of binging on ice and of injecting methylamphetamine among Queensland ecstasy and psychostimulant users is of particular concern.

Role of organised crime in the methylamphetamine market in Queensland

The ACC has reported that organised crime groups are increasingly becoming involved in the methylamphetamine market within Australia. While many of these groups traditionally focused their attentions on heroin and cocaine—and on the importation of these substances with a view to making money—many are now moving to include methylamphetamine in their pursuits.256

The reasons for this move are varied, but it is widely recognised that the methylamphetamine market in Australia is extremely lucrative and that the market for the purchase of this drug is growing throughout the country.
Within Queensland, the CCC in its submission to this Inquiry noted that ‘[i]ntelligence collected from a range of sources indicates an increase in the prevalence of crystal methylamphetamine (ice) in Queensland and entrenched criminal activity in this market.’ The CCC further notes that ‘[t]he increased demand for ice is attracting greater involvement of organised groups due to the profits available in the market.’

As at June 2015, indicative figures drawn from Queensland Police Service (QPS) intelligence reveals that 76 per cent of identified Queensland organised crime networks are involved in the illicit drug market, with 51 per cent linked to methylamphetamine.

Further, it is not just organised crime groups located within Queensland or even Australia that are penetrating the industry. Rather, transnational organised crime groups are more involved in the methylamphetamine industry in this country than ever before.

The ACC has suggested that recent increased border detections of methylamphetamine, in conjunction with continued high incidences of local clandestine laboratory detections, indicates an increased interest from transnational organised crime groups, who may have recognised the high demand for the drug in Australia and identified it as a lucrative market.

The ACC noted that:

Transnational organised crime involvement in the Australian methylamphetamine and precursor markets is entrenched, and will likely expand in the medium term. The highly lucrative nature of the Australian market, combined with the availability and relatively low cost of methylamphetamine and precursors internationally, will sustain this involvement.

In the same report, the ACC notes that more than 60 per cent of the entities on the National Criminal Target List (a list which identifies nationally significant organised criminal syndicates and individuals impacting on Australia) are involved in methylamphetamine and/or precursor markets.

It is evident that organised crime groups continue to develop new ways of manufacturing methylamphetamine. As they do this, they also attempt to exploit chemicals that are not regulated or controlled, in order to assist in the production of methylamphetamine.

While the introduction in 2006 of controls over the use of precursor chemicals within Australia—particularly pseudoephedrine—assisted in the decrease of the use of those particular products in the manufacturing process within Queensland, organised crime groups have been sourcing chemicals from overseas to enable the production of methylamphetamine. This has resulted in an increase in the growth of methylamphetamine use since 2009.

The CCC, in its submission to the Inquiry, noted that:

... organised crime groups traditionally involved in heroin trafficking have expanded their activities to become involved in the trafficking of methylamphetamine as well as precursor chemicals to take advantage of these growing markets ... The ability for organised crime groups to reliably source pseudoephedrine to manufacture methylamphetamine has been affected by domestic market regulation, but there is evidence that organised crime groups have adapted to these regulations and a distinct illicit market for precursor chemicals has evolved.

One example of such precursor chemicals being sourced from overseas was the drug ‘ContacNT’. ContacNT is a cold and flu medication which was known to contain a very high concentration of pseudoephedrine and was, until recently, easily available to purchase in and from China. Prior to 2009, detections of this drug at the Australian border were limited; however, detections increased following the introduction of ‘Project STOP’ in Australia. Project STOP made it more difficult to purchase pseudoephedrine products domestically.

Detections of ContacNT increased from 20.4 kilograms in 2009 to over one tonne in 2011–2013. The Chinese government has recently regulated ContacNT so that it is not as readily available. In late 2012, China began requiring identification for people buying cold medicine containing ephedrine and pseudoephedrine as well as rationing the amount that can be purchased by consumers. In certain circumstances where the proportion of pseudoephedrine is higher, a prescription from a doctor is also required.
In Queensland, four laboratories devoted to the extraction of pseudoephedrine from other materials were detected in 2013–2014, indicating that this is still a popular method of producing methamphetamine.266

According to the UNODC, as more and more controls are placed on precursor chemicals, international organised crime groups have emerged that specialise in precursor chemicals.267 Another method of evading international controls has been diversifying to use a broader range of non-controlled chemicals to allow crime groups to manufacture precursors required for methamphetamine production.268 For example, in North America, Central America and Europe, the precursor 1-phenyl-2-propanone (or ‘P-2-P’) is used to make ‘methamphetamine’.269 P-2-P is subject to international—and in many places national—controls.270 Recently, traffickers have been using substances that are not controlled, such as benzyl cyanide, sodium salts of P-2-P glycic acid, benzaldehyde, and esters of phenylacetic acid to produce P-2-P, which is subsequently used to produce methamphetamine.271 This is just one of many examples of non-controlled ‘pre-precursors’ being used to circumvent precursor-controlling regimes.272

In addition to the exploitation of unregulated and uncontrolled chemicals being imported from overseas, there continues to be a problem within Australia of diversion of chemicals from legitimate sources. The ACC notes that there have been several instances in which organised crime group members or their associates have established a chemical-related business with the intention of appearing legitimate and using it as a cover for purchasing precursors.273

In relation to the domestic production of methamphetamine—which traditionally has been sufficient to supply the local market—it seems there is a trend away from this. The CCC has indicated that:

Since 2010 there has been a considerable increase in methamphetamine detections at the border. Further, QPS has reported a decrease in the detection of clandestine laboratories in the past twelve months (approximately 30% decrease). This could be indicative of organised crime groups becoming increasing involved in the importation of high purity ice to meet the demands for this substance.274

Detective Inspector Mark Slater of the QPS Drug Squad confirmed this in his interview with the Commission. He noted that, in relation to ice, his experience was that nearly all of it was imported.275

Organised crime is clearly heavily entrenched in the methamphetamine market within Queensland. It is expected that it will continue to thrive in an environment where there is a high demand for the product, where the purity is increasing, and where the user is finding the drug easier to obtain than previously. This drug has justifiably been assessed as being of a very high risk factor to the Australian community and posing the greatest threat of any drug to our society.

Conclusion

It is clear from research undertaken that methamphetamine is of great concern and poses the greatest risk to the Queensland community276 due to a number of reasons:

1. the increase in availability of methamphetamine
2. the growth in the use of crystal methamphetamine (ice)
3. the increasing use of methamphetamine in regional and remote communities
4. the fact that not only is methamphetamine produced locally, but a much higher amount is being imported from overseas
5. the increase of methamphetamine’s purity
6. the fact that more than 60 per cent of Australia’s highest-risk criminal targets—including transnational targets—are involved in the methamphetamine market
7. the extreme dangers to the individual, the community and the economy as a result of the consumption of this illicit drug.

The greatest concern to the Queensland community in relation to methamphetamine use should be the drug ice. There has been a dramatic increase in the number of people using this drug, which has a significantly higher purity than traditional methamphetamine. The violence associated with the use of
The illicit drug market affects not only the user, but the wider community, in a variety of ways. This problem is not only confined to Queensland, but has been recognised nationally—resulting in the National Ice Taskforce. This Taskforce is currently in the process of working with state bodies to develop the National Ice Action Strategy. Given that the use of methylamphetamine in Queensland is higher than the national average, Queensland must take an active role in the establishment and implementation of this strategy. It is necessary that the state have a plan in place to tackle this most concerning type of methylamphetamine.

(Endnotes)


The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry

detailed report (Drug statistics series No. 28). Canberra: Commonwealth
Government, table 5.19 – 14.1 per cent of
recent methylamphetamine/amphetamine
users had used prescription amphetamines
while 71.5% used ice, 64.9 per cent used
powder, 28.3 per cent used base and 26.5
per cent used tablets.

37 See for example, United Nations Office
on Drugs and Crime. (2014). World Drug
Drug Data Report 2012–13. Canberra:
Commonwealth Government, p. 156.

38 United Nations Office on Drugs and Crime.
United Nations, p. 73.

39 United Nations Office on Drugs and Crime.
United Nations, p. 73.

40 United Nations Office on Drugs and Crime.
United Nations, p. 75.

41 Crime and Corruption Commission.
Brisbane: Queensland Government, p. 42
[In Confidence].

Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

44 United States National Institute on
Drug Abuse. (2014). Drug Facts
Methamphetamine. Maryland: United States
drugabuse.gov (accessed 18 August 2015).

45 Jenner L. and Lee N. (2008)
Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

46 Jenner L. and Lee N. (2008)
Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, pp. 15–16.

Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

48 United States National Institute on
Drug Abuse. (2014). Drug Facts
Methamphetamine. Maryland: United States
drugabuse.gov (accessed 18 August 2015).

49 Jenner L. and Lee N. (2008)
Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 16.

50 Jenner L. and Lee N. (2008)
Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 16.

Patterns and consequences of the use
of amphetamine-type stimulants (ATS):
Technical Briefs on amphetamine-type
stimulants (ATS) 1. Philippines: World
Health Organization.

52 United States National Institute on Drug
Abuse. (2013). Methamphetamine: Research
Report Series. Maryland: United States
drugabuse.gov (accessed 18 August 2015).

Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

54 Jenner L. and Lee N. (2008)
Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

Treatment Approaches for Users of
Methamphetamine: A Practical Guide
for Frontline Workers. Canberra:
Commonwealth Government, p. 15.

56 Sydney Morning Herald. (2014). Ice – the
drug that’s hard on the head and hard
on families. Available at http://www.smh.
com.au (accessed 19 August 2015) [relying
on quotation of Associate Professor
Nicole Lee, of the National Centre for
The illicit drug market


The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry


<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>

**The illicit drug market**

**Queensland Organised Crime Commission of Inquiry**

56
The illicit drug market

Queensland Organised Crime Commission of Inquiry


The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry


The illicit drug market

The illicit drug market

Queensland Organised Crime Commission of Inquiry


The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry


257 Submission of Crime and Corruption Commission, 22 May 2015, p. 8 [In Confidence].

258 Letter from Crown Law on behalf of Mr Michael Byrne QC, A/DPP, 3 August 2015 [In Confidence].


262 Submission of Crime and Corruption Commission, 22 May 2015, p. 8 [In Confidence].


Commonwealth of Australia, table 37, p. 166.


275 Transcript of Interview, Mark Slater, 1 July 2015, p. 4 [In-Confidence].

3.2.2 Cocaine

The drug and its effects on the user

Under Queensland’s Drug Misuse Act 1986 and Drugs Misuse Regulation 1987, cocaine is a prohibited drug, and the unlawful possession, production and supply of, and trafficking in the drug is a crime.

Cocaine is a highly addictive stimulant drug. It affects the user by stimulating the central nervous system, speeding up the messages between the body and the brain. After taking the drug, cocaine users experience a number of short-term effects, including feeling happy, confident, energetic, alert, talkative, strong, contemplative and full of rapture. They may also experience an increased sex drive.

Cocaine is extracted from the leaves of the South American coca bush. There are two species of coca bush that are used to produce cocaine: *Erythroxylum coca*, which has the highest cocaine content, and *Erythroxylum novogranatense*. Coca bush is predominantly grown in Colombia.

Cocaine is extracted from the leaves of the coca plants by soaking them in solvents to produce a paste. The paste is then treated with hydrochloride acid and dried to produce a salt form. This form of the drug appears as a white powder. This type of cocaine is commonly snorted by users or dissolved in water and injected. It is sometimes rubbed into gums or ingested with drinks and food, but it is not suitable for smoking.

This type of cocaine is sometimes called ‘cocaine hydrochloride’, and it is the main form of the drug used in Australia.

Cocaine in this form is often mixed, thinned, or ‘cut’ with other substances to increase its weight and reduce its purity. This can increase the risk of overdose as users may not know the strength of the powder they are ingesting. Some of the substances cocaine is cut with include lactose, sugar, talcum powder, baking soda and glucose. Recently, levamisole—a drug used in the agriculture industry to treat worms and parasites in livestock—has been detected in seized cocaine. The inclusion of levamisole presents additional health risks to cocaine users.

In addition to being ‘cut’ with these substances, cocaine hydrochloride is sometimes also mixed with other illicit substances, such as heroin, and injected. This practise is known as ‘speed-balling’, but it is uncommon in Queensland.

Cocaine in the hydrochloride salt form can be further treated to produce ‘freebase’ cocaine. Freebase cocaine can come in a white powder, a crystallised form or as small lumps or ‘rocks’. The crystal or rock form is commonly known as ‘crack’ cocaine. These forms of cocaine are usually smoked, but they are uncommon in Australia.


It is typically associated with drug users from a higher socio-economic status than other illicit drug users. User groups often consist of educated professionals, wealthy socialites, sporting identities and social drug users who are less likely to come into contact with law enforcement in their daily lives.

In Queensland, cocaine is listed as a dangerous drug in Schedule 1 of the Drugs Misuse Regulation. Accordingly, trafficking (section 5), supplying (section 6), producing (section 8) or possessing (section 9) the drug is punishable under the Drugs Misuse Act with maximum penalties of 15 years, 20 years, 25 years, or life imprisonment, depending upon the particular circumstances and weight involved.

Effects of cocaine on the user

Cocaine causes a ‘rush’ or ‘high’ feeling because of the way it interacts with the brain. Although cocaine interacts with the brain in a number of ways, its most significant impact is how it affects a chemical called dopamine. Dopamine is a neurotransmitter in the brain that causes a sense of pleasure and satisfaction as a rewarding mechanism. The use of cocaine increases the amount of dopamine in the brain, which in
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Turn causes feelings of euphoria and makes the user want to take the drug again. This effect can lead to a dependence on the drug, and users may crave the drug to experience the pleasure again, or they may become reliant on the drug to feel pleasure.

These effects of cocaine are generally short-lasting, although the way in which a person uses cocaine may impact the duration of its effects. When cocaine is either smoked or injected, it enters the bloodstream and the brain rapidly. This means that the user feels the effects quickly, but the effects may only last a short amount of time, such as five to 10 minutes. People who snort cocaine have to wait longer to feel the effects of the drug, but the sensation may last longer, with some reporting a duration of 15 to 30 minutes. The short duration can lead to a person re-dosing within a small timeframe to re-experience the ‘high’, which can, in turn, increase the risk of dependency and overdose.

Although health issues related to cocaine are not as pronounced as some other illicit drugs, cocaine use can present a number of serious risks to the health of users.

Short-term effects of cocaine

In addition to the euphoric effects that cocaine can have on the user, it can also induce a number of negative short-term effects, particularly when taken in high doses. Some of these effects include: paranoia, anxiety, panic, hallucinations, agitation, violent or aggressive behaviour, dry mouth, reduced appetite, nausea, abdominal pain, vomiting, indifference to pain, headaches, increased blood pressure, faster breathing (after first slowing down), increased or disturbed heartbeat, increased body temperature, chest pain, tremors, seizures, kidney failure, stroke, heart attack, and, in some instances, death.

Long-term effects of cocaine

In addition to the adverse effects of short-term use and overdose, there are also a number of long-term health consequences of cocaine use. These include: insomnia, exhaustion, depression, anxiety, paranoia, psychosis, aggression, mood swings, weight loss, eating disorders, impaired sexual performance, kidney failure, high blood pressure, sensitivity to light, sensitivity to sounds, hallucinations, impaired cognitive function, irregular heartbeat, inflamed or enlarged heart muscle or heart disease, which may in some instances cause death. Long-term use of cocaine can also cause dependency.

Accidental death from cocaine overdose

In Australia, deaths from cocaine overdose are relatively rare when compared with other illicit drugs. In 2011, there were nine deaths attributed to cocaine in the 15–54 year old age group, in comparison to 21 deaths attributed to methylamphetamine and 201 deaths attributed to heroin overdose in the same age group. However, this is the highest number of deaths caused by cocaine since 2005, and the second-highest number of deaths due to cocaine during the period between 1997 and 2011.

Despite the relatively low number of deaths, cocaine still presents a risk to users, particularly because toxic reactions to cocaine are not necessarily dependent on the size of the dose, the frequency of use or the manner in which it is used. However, the risk of overdose is likely to increase where cocaine is administered through injection.

Deaths from cocaine are most commonly the result of seizures, respiratory failure, cardiac arrhythmia (when the heart beats too fast or irregularly, which can result in an insufficient blood supply to the brain), or hyperthermia (when the body gets too hot and causes organ failure). Some studies have shown that cocaine users are 14 times more likely than non-users to have suffered from a stroke in their lifetime.

Effects of the method of consumption of cocaine

The way in which a person uses the drug may cause additional health problems for the user. Use of the drug through injection is particularly risky, as it may compromise the health of a user when needles are dirty, reused or shared. Poor needle practises can result in the cocaine user contracting tetanus, hepatitis B, hepatitis C, human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome (AIDS). These conditions are serious and, in some instances, chronic and life-threatening.
Injecting cocaine can also cause vein damage, abscesses on the skin, and bacterial infections that can damage the heart and its valves.50

These injection-related issues appear to be more common among injecting users of cocaine than among injecting users of other illicit drugs, like heroin.51 This is because cocaine has short-lasting euphoric effects, resulting in more frequent injecting than other drugs.52

Although uncommon in Australia, the smoking of cocaine can also have particularly detrimental effects on the user. Cocaine can damage the lungs and affect the respiratory system.53 It may cause a cough, bloody or black sputum or phlegm, wheezing, shortness of breath, and chest pain.54 It can also cause tooth decay and grinding.55 Those who smoke cocaine are also more likely to become dependent upon the drug than those who snort it.56

Snorting cocaine can cause congestion, a runny nose or nose bleeds, nasal septum perforation (a hole in the part of the nose that separates the left and right airways), ulcers in the nasal septum, sinus problems and a loss of the sense of smell.57

**Effect of ‘fillers’ and other drugs**

Cocaine users are also exposed to health risks as a result of ingesting other materials that have been mixed with cocaine. Recently, a substance called levamisole has been detected in cocaine in Queensland.58 This substance has been associated with agranulocytosis, which is a deficiency in white blood cells resulting in a suppression of the body’s immune system.59 This means that common infections may become life-threatening.60 Levamisole has also been associated with fatigue, joint pain, lung problems, skin problems, and seizures.61

Additionally, when cocaine is used in association with other drugs, the risks to the user are increased. When used with alcohol, the combination may cause liver or heart failure.62 When cocaine and heroin are used together, there is an increased risk of problems with the respiratory system, which may lead to the user falling into a coma.63

**Dependency and withdrawal**

Cocaine is a highly addictive drug.64 Due to the way in which cocaine interacts with dopamine in the brain, a user feels ‘rewarded’ for using the drug.65 This encourages people to repeat that behaviour, which can create a dependency or addiction.

The more the drug is used, the more the brain adapts to the release of large amounts of dopamine. It can compensate by producing less dopamine, or by reducing the receptors in the brain that react to the dopamine.66 This means that people keep using cocaine, or higher doses of cocaine, to get the same euphoric effects that they previously had from the drug.67 This also means that other activities outside of drug use that would normally bring pleasure become less enjoyable.68

The short-lasting effects of cocaine can also cause a person to ‘re-dose’—or binge—within a short amount of time, thus increasing the risk of dependency.69

When a user has become dependent on cocaine, they may have some or all of the following symptoms and habits:

- They may be tolerant to the euphoric effects of cocaine.
- They may require higher dosages of cocaine to achieve the desired effect.
- They may use cocaine in large amounts whenever it is available, without saving any for later use.
- They may be unable to reduce the amount of cocaine they are using.
- They may spend most of their time and energy obtaining or using cocaine.
- They may engage in other unlawful activities, such as theft and burglary, to obtain money to buy cocaine.
They may continue to use cocaine, despite knowing that they may develop—or actually suffering from—adverse physical and mental health consequences.70

Another sign of dependency is the presence of withdrawal symptoms when a person is unable to obtain cocaine, or if they cease using cocaine.71 These symptoms include: cravings, tiredness, weakness, disturbed sleep, depression, nausea, vomiting, shaking, hunger, muscle pain and, in some circumstances, suicidal thoughts.72

Addiction to the drug may make it difficult for a user to maintain employment due to absenteeism or ineffectiveness while at work, and may isolate them from friends and family.73 Dependency on the drug can also increase the risks of adverse long-term health effects.

Despite its addictive nature, many Australians do not become dependent on the drug. This is evident from the high number of cocaine users that report only using the drug once or twice a year.74 This is much less frequent use than that of other illicit drugs like cannabis, ecstasy and ‘meth/amphetamines’.75 Given the negative health and social impacts that cocaine dependency can have on an individual—and incidentally, the community—this is at least one positive aspect of cocaine use in Australia.

Cocaine health-related issues in Queensland

In Queensland, the harms associated with cocaine use are relatively low when compared with other illicit drugs. In 2013–2014, there were 27 attendances by Queensland Ambulance Service where cocaine was the primary drug of concern, which was a decrease from 42 in 2012–2013.76

Hospital admissions with a principle diagnosis relating to cocaine in Queensland in 2013–2014 were also relatively low, at nine admissions per million, equating to approximately 22 admissions for that year.77 This compares to 227 hospital admissions per million persons for methylamphetamines78 and 463 admissions per millions persons for opioid-related treatment for that year.79 Nationally, there were 28 hospital admissions with a principle diagnosis relating to cocaine per million in 2012–2013.80

The Crime and Misconduct Commission, as it then was, attributed the lower rate of harm associated with cocaine use in 2012 to its relatively low injection rates, the absence or rarity of crack cocaine in the Queensland market, the infrequency of cocaine consumption among its user group, and the generally low numbers of users.81

The prevalence of cocaine within the community

Globally, cocaine was estimated in 2013 to be used by between 13.8 million and 20.7 million people.82 This equates to approximately 0.3 to 0.4 per cent of the global population.83 Use of cocaine was higher in North America, Oceania, South America, and Western and Central Europe, with a greater proportion of those populations using cocaine than people in other regions.84 It is surprising, given the high levels of cultivation of the coca plant in South America, that a higher proportion of the population in Oceania uses cocaine than that of the population in the drug’s originating region.
North America has the highest total number of cocaine users, with approximately 5.2 million people taking the drug there in 2013. This was followed by South America (3.3 million users), Western and Central Europe (3.1 million users), and West and Central Africa (1.6 million users). Although Oceania had one of the highest rates of cocaine use among its population, it only had the eighth-highest number of users, due to its smaller population size. For the purposes of cocaine use in the World Drug Report 2015, ‘Oceania’ refers only to use in Australia and New Zealand, as other statistics were not available.
According to the United Nations Office on Drugs and Crime (UNODC) best estimates, in 2013, cocaine was used less commonly globally than cannabis, amphetamines, prescription stimulants and opioids. Despite this, cocaine appears to have a foothold in a number of illicit drug markets across the world.

The high levels of cocaine use in Oceania are mostly attributable to the popularity of the drug in Australia. Australian habits in this regard will be considered further below.

The largest growers of the cocaine bush are the Plurinational State of Bolivia, Peru, and Columbia. The area dedicated to growing coca bush for cocaine has decreased recently, which caused a global decrease in the production of cocaine. It has been estimated that as of 31 December 2013, there were approximately 120,800 hectares of land dedicated to growing the plants globally. This was a decrease of approximately 10 per cent from 2012. Cultivation has been decreasing since a peak in 2007 (see Table 3), with 2013 the lowest level since estimates in the mid-1980s.

Cocaine hydrochloride is also predominantly produced in South America. Typically, farmers of the coca plants sell the coca leaf or the paste extracted from the leaves to local laboratories. In some instances, the farmers may operate these laboratories themselves. These laboratories then sell either the paste or the cocaine hydrochloride to transnational drug trafficking groups. Previously, it was common practice for growers in Peru and the Plurinational State of Bolivia to send their coca paste to Colombia to be further processed into cocaine hydrochloride. However, by 2008, Peru and the Plurinational State of Bolivia were responsible for manufacturing approximately half of the world’s finished cocaine supply. Cocaine processing laboratories have also been located in Argentina, Chile, Ecuador and Venezuela. Cocaine used in Australia is generally of either Colombian or Peruvian origin, with very few seized samples indicating an origin in the Plurinational State of Bolivia.
It is difficult to rationalise the global position regarding cocaine. In some countries, use is decreasing, while in others it is becoming more popular. In 2010, UNODC noted that global annual use had remained stable at around 0.4 per cent of the adult population between 1998 and 2008. A review of the estimated rates of use globally between 2009 and 2013 indicates continued stability in the global market, at about 0.4 per cent of the global population each year. Although the amount of land being used to grow coca bush is decreasing, it does not appear that there has as yet been any significant shortages of cocaine supply, or any substantial decrease in its use.

### The prevalence of cocaine in Australia

Cocaine is one of the most popular illicit drugs in Australia. In 2013, an estimated 400,000 Australians recently used cocaine, which is approximately 2.1 per cent of the population. In that same year, approximately 1.5 million Australians had tried cocaine at some point in their life, which is 8.1 per cent of the population.

In 2013, cocaine was the third most popular illicit drug used by Australians, behind cannabis and ecstasy. It shared this position with ‘meth/amphetamine’ (defined in the national survey as including both methylamphetamine and amphetamines), which had equal levels of recent use in the community. A greater proportion of the population had used cocaine in the previous 12 months in 2013 than had used heroin, hallucinogens, GHB, cannabimimetics, or drug analogues and new psychoactive substances.

In 2013, Australians were more likely to have tried cocaine in their lifetime than they were to have tried ‘meth/amphetamines’, heroin and inhalants. In recent years, the proportion of people who are likely to have tried cocaine in their life overtook the proportion of those ever trying ‘meth/amphetamines’.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Meth/amphetamine and cocaine - % of Australian population using in past 12 months and over their lifetime


Although recent use in Australia remained stable between 2010 and 2013, a greater proportion of the population reported having an opportunity to use cocaine in 2013 than they did in 2010. This is consistent with findings from a national survey of ‘ecstasy’, psychostimulant and injecting drug users, in which users indicated that cocaine was ‘easy’ or ‘very easy’ to obtain in higher proportions than those reporting that it was difficult or very difficult to obtain.

Cocaine is a particularly expensive drug to use, and the drug is commonly associated with affluence. In 2013–2014, the prices for cocaine ranged from between $250 and $1,000 per gram, according to the ACC. A 2014 study of ‘ecstasy’ and psychostimulant users that had purchased cocaine found that the national median price paid by those users was $300 a gram. In that same study, those who had used cocaine in the past six months reported a median use of half a gram for an average using ‘episode’.

When compared to other drugs such as MDMA/‘ecstasy’, the high price of cocaine is clear. For example, in the Ecstasy and Related Drugs Reporting System report in 2014, participants in the study reported using a median of two ‘ecstasy’ tablets in a typical session. Having regard to the national median cost of the tablets, this would amount to $50 a session. In comparison, to cocaine users reported using half a gram per typical session, which would amount to approximately $150 a session.

The high cost of cocaine may be one of the reasons the cocaine-using population differs from other groups of illicit drug users. In 2013, use of cocaine was most common among those with the highest socio-economic status in Australia.

Not only was the drug most popular among the group with the highest socio-economic status, but use of the drug also increased in popularity as socio-economic status increased. This pattern is not always seen
in drug users; for example, both cannabis and ‘meth/amphetamine’ are most popular among people of an average socio-economic status and less popular among those with a higher socio-economic status.120 ‘Ecstasy’ also has higher use among those with a high socio-economic status, but the difference between the prevalence of use among the most advantaged and least advantaged is not as marked as it is with cocaine.121

Recent (past 12 months) illicit drug use among socio-economic groups

![Graph showing illicit drug use among socio-economic groups](image)


The use of cocaine in Australia is also slightly more common in major cities than it is in remote and very remote areas, unlike cannabis and ‘meth/amphetamine’.122 This is consistent with its use by those of a high socio-economic status. Although historically, cocaine use was associated with Victoria and New South Wales,123 the most recent National Drug Strategy Household Survey indicated that cocaine use in 2013 was most prevalent in the Australian Capital Territory, followed by New South Wales and then the Northern Territory.124 Cocaine use in Queensland is as prevalent as Victoria.125

In addition to being more likely to reside in major cities, recent cocaine users in Australia were also more likely to be men than women, and in the 20–29 year age group.126 The median age of recent cocaine users was 29, which is older than that of users of ‘meth/amphetamine’, ‘ecstasy’ and hallucinogens, but younger than that of cannabis and heroin users.127 The median age has increased from 25 in 2001, indicating an aging cohort of cocaine users.128 There was also a rise in the proportion of men aged 40 years and older using cocaine in 2013 from 2010.129

 Australians between 14 and 24 years old are generally introduced to cocaine at 19.2 years of age.130 This is an older initiation age than cannabis, ‘ecstasy’, ‘meth/amphetamines’, heroin and hallucinogens.131 This age has
been stable since 2010, but is an increase from 17.1 years in 1995.\textsuperscript{132} The fact that initiation into the drug is older than for other illicit drugs may be due to the high cost of cocaine.

Cocaine users 18 years and above are less likely to use the drug frequently than other types of drug users. Of those who used cocaine recently in 2013, 71.3 per cent reported use once or twice a year.\textsuperscript{133} This use was less frequent than those who reported recently using cannabis, ‘ecstasy’ or ‘meth/amphetamine’.\textsuperscript{134} This was also less frequent use of the drug by recent users than in 2010.\textsuperscript{135}

**Frequency of illicit drug use among recent (past 12 month) users aged 18 years and above in 2013**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Cannabis</th>
<th>Ecstasy</th>
<th>Meth/amphetamine</th>
<th>Cocaine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every day</td>
<td>80.00%</td>
<td>70.00%</td>
<td>60.00%</td>
<td>50.00%</td>
</tr>
<tr>
<td>Once a week or more</td>
<td>10.00%</td>
<td>20.00%</td>
<td>30.00%</td>
<td>40.00%</td>
</tr>
<tr>
<td>About or at least once a month</td>
<td>0.00%</td>
<td>20.00%</td>
<td>50.00%</td>
<td>20.00%</td>
</tr>
<tr>
<td>Every few months</td>
<td>0.00%</td>
<td>10.00%</td>
<td>20.00%</td>
<td>10.00%</td>
</tr>
<tr>
<td>Once or twice a year</td>
<td>0.00%</td>
<td>10.00%</td>
<td>20.00%</td>
<td>40.00%</td>
</tr>
</tbody>
</table>


Despite its common association with the wealthy, those users who inject the drug typically come from a lower socio-economic background than those who snort the drug.\textsuperscript{136} However, cocaine is one of the least popular illicit drugs among injecting drug users, with only 12 per cent of users participating in the Illicit Drug Reporting System in 2014 stating that they used cocaine in the preceding six months.\textsuperscript{137} This compared to 70 per cent reporting use of any form of methylamphetamine 60 per cent reporting use of any form of heroin and 73 per cent reporting use of cannabis.\textsuperscript{138} This was a slight decrease from 2013, and is consistent with a decrease in popularity of the drug among injecting drug users since 2001.\textsuperscript{139} Of the 12 per cent that had recently used cocaine, the majority had taken it through injection.\textsuperscript{140}

Despite being relatively unpopular among injecting drug users, cocaine use appears to be increasing in popularity among other drug-using groups. Cocaine use in those who use ‘ecstasy’ and other psychostimulants increased in 2014, with 44 per cent of participants in a national study of ‘ecstasy’ and psychostimulant users reporting use of cocaine in the past six months.\textsuperscript{141} This was an increase from 36 per cent reporting cocaine use in the past six months in 2013.\textsuperscript{142} It is unclear at this stage whether the increase in use by ‘ecstasy’ and psychostimulant users will be mirrored by an increase in use among the community generally.

The amount of cocaine seized at the Australian borders decreased in 2013–2014 from 399.6 kilograms in 2011–2012 to 245.6 kilograms.\textsuperscript{143} This is the lowest amount of cocaine detected since 2005–2006.\textsuperscript{144} All of the significant seizures made in 2013–2014 were destined for Sydney.\textsuperscript{145} It is unclear whether this indicates a lower
supply of cocaine to the country, less demand for the drug, or whether traffickers are simply using more sophisticated importation techniques.

The seizures indicated that cocaine is being sent to Australia from 50 countries, with Canada being the most common embarkation point in 2013–2014. Cocaine was also commonly sent from Chile, Brazil, the United States of America, Argentina, Colombia, Peru, Malaysia, South Africa, the United Arab Emirates, and Trinidad and Tobago.

In Australia, use of cocaine has remained stable between 2010 and 2013, but cocaine has generally increased in popularity since 1993. Although use has been stable in the last few years, it appears that the drug is becoming more available, with more people reporting that they had been offered—or had an opportunity to use—cocaine in 2013 than in 2010. Despite this availability, users are turning to the drug less frequently. There also appears to be less uptake of the drug among younger members of the community. Nevertheless, the drug remains a concern given its continuing popularity in the Australian community.

The prevalence of cocaine use in Queensland

In Queensland, cocaine use is slightly below the national average, but the popularity of the drug is increasing. In 2013, two per cent of the Queensland population had used cocaine in the past 12 months. Queensland had the fourth-highest proportion of the population reporting recent cocaine use, along with Victoria.

% of population using in the last 12 months 2013

![Cocaine Use Percentage Chart]


Despite cocaine being as popular as ‘meth/amphetamine’ nationally, in Queensland, people were more likely to have recently used ‘meth/amphetamine’. This means that cocaine is the fourth-most commonly used illicit drug in the state (not including pharmaceuticals), behind cannabis, ‘ecstasy’ and ‘meth/amphetamine’.

According to the CCC, use of cocaine in Queensland is increasing. This position is supported by the results of the National Drug Strategy Household Survey 2013, which indicated that although the national prevalence of cocaine remained stable at 2.1 per cent in 2010 and 2013, use in Queensland rose from 1.3 per cent in 2010 to 2 per cent in 2013. In the same period, use in New South Wales remained stable, and use in Victoria, Western Australia and South Australia dropped.

There is limited data available on cocaine use in Queensland. This is, in part, due to the fact that cocaine users are primarily from a group of wealthier users, who do not regularly come into contact with law enforcement. In this regard, the cocaine market is somewhat ‘hidden’ from the general population and law enforcement agencies.

The CCC has, however, recently noted that there is a broadening cocaine user group at the Gold Coast. There have also been some examples of an increase in the demand for the drug in regional areas of Queensland. In one instance, police intercepted a motor home and charged a person who was found to be
The illicit drug market

Infrequent use of the drug also appears to be a using pattern in Queensland, with a recent study on ‘ecstasy’ and psychostimulant users indicating that Queensland participants who had recently used cocaine had used it on a median of two days in the past six months.\textsuperscript{158} For Queensland injecting drug users recently using cocaine, the median was one day in the six months before they participated in the study.\textsuperscript{159}

This pattern was also observed in a review of wastewater from the Gold Coast area in 2012. The review involved collecting of untreated wastewater and using chemical analysis to determine the concentrations of certain licit and illicit substances in the wastewater, which has been excreted in urine, faeces, saliva and sweat.\textsuperscript{157} When a substance is consumed, it is usually discharged from the body in these ways within 24 hours of a person consuming drugs.\textsuperscript{160} The analysis found that the presence of cocaine in the wastewater increased around major events and festivals. This supports the Crime and Misconduct Commission’s 2012 view that cocaine was a ‘special occasion’ drug.\textsuperscript{162} Recent wastewater analysis has also indicated that there has been a more general trend of increased daily usage of cocaine in the Gold Coast area since January 2012.

The high prices of cocaine could explain the infrequency of the drug’s use in Queensland. In Queensland, the median price paid by those recently buying cocaine in a study of the drug use patterns of ‘ecstasy’ and psychostimulant users was $300 a gram, which was consistent with the national average.\textsuperscript{163} Those injecting the drug reported slightly higher median price of $350 per gram, which was also consistent with the national median for that user group.\textsuperscript{164} The CCC has noted that some of the inhibitors of the Queensland cocaine market are its high price and short-lasting effects.\textsuperscript{165}

Cocaine in Queensland is predominantly sourced from Sydney and Melbourne, and originates in South America.\textsuperscript{166} There have, however, been some instances of cocaine being imported into Queensland via small vessels.\textsuperscript{167} In 2010, one shipment was detected in Brisbane carrying approximately 400 kilograms of cocaine, and in 2011, a vessel was detected in Bundaberg carrying approximately 300 kilograms of the drug.\textsuperscript{168}

Seizures of cocaine may shed some light on the demand for the drug in Queensland. In 2013–2014, there were 13.8 kilograms of cocaine seized by law enforcement agencies, which was an increase from approximately 4.5 kilograms in 2012–2013.\textsuperscript{169} This is, however, a significant decrease from approximately 295 kilograms seized in 2011–2012 and 402 kilograms seized in 2010–2011.\textsuperscript{170} Information from the Crime and Misconduct Commission (as it then was) indicates that the two intercepts described above would account for these high seizures in 2010–2011 and 2011–2012. Given the number of people reporting use of the drug in Queensland in 2013, it does not appear that a reduction in the amount of cocaine seized is directly related to the level of demand for the drug in the state.

As there is limited data on cocaine use, arrest figures in Queensland may also assist in determining trends in cocaine use. Arrests for cocaine supply and possession offences have steadily increased in the state over the past four years, which is consistent with a growth in use of the drug and national arrest rates.\textsuperscript{171}

Although the national rate of cocaine use is remaining stable, the drug is increasing in popularity in Queensland. This could increase the number of people with cocaine-related medical conditions and emergencies, and present new challenges for law enforcement agencies in the state.

The nature and extent of organised crime in the Queensland cocaine market

Organised crime plays a large role in the global cocaine market. Entrenched international crime groups from Colombia and Mexico have long dominated cocaine trafficking.\textsuperscript{172} Although the market has traditionally been associated with Colombian crime groups, law enforcement efforts and the threat of extradition to the United States has minimised the role of these groups in large-scale cocaine trafficking, particularly to the United States, since the 1990s.\textsuperscript{173} However, these groups still play a role in selling the drug to other groups for further distribution.\textsuperscript{174}

Mexican cartels have emerged in importing and distributing cocaine, particularly in the United States.\textsuperscript{175} These cartels have demonstrated a propensity toward extortion, kidnapping and other forms of acquisitive crime.\textsuperscript{176}
New trafficking routes that have opened up in response to law enforcement activities and other factors have also exposed to the cocaine market criminal groups that had not previously been associated with the drug.\(^{177}\) In the 2013 Organised Crime in Australia report, the Australian Crime Commission (ACC) predicted that more of these new groups would become involved in trafficking cocaine to and in Australia, as there is a lucrative market here for the drug.\(^{178}\)

Although there have traditionally been limitations on the growth of the market in Australia due to the low purity of the drug and the high costs, the popularity of cocaine has increased since the early 1990s.\(^{179}\) Like in the United States, Mexican organised crime groups have been identified as playing a role in importing cocaine into Australia.\(^{180}\) Criminal entities with links to these markets were, at least as of 2012, thought to be responsible for most of the large-scale importations into Australia from Mexico.\(^{181}\) It has been suspected that one of the methods used to import cocaine into Australia is to send it from Mexico to Canada, and then forwarded to Australia.\(^{182}\) This could explain why Canada was the most common embarkation point of intercepted cocaine in 2013–2014.

The Commission is aware of organised crime groups from other ethnic backgrounds that have also been identified as being involved in trafficking cocaine in Australia.

The majority of cocaine on the Queensland market is sourced from Sydney and Melbourne.\(^{183}\) However, the Crime and Misconduct Commission, as it was then, reported in 2012 that transnational and Australian-based crime groups were targeting regional areas of Queensland to import and store cocaine and other drugs for later distribution in Sydney and Melbourne.\(^{184}\) It was believed that this strategy was being employed to avoid the high levels of attention that the main criminal networks in capital cities receive from law enforcement agencies.\(^{185}\)

The Commission is aware of a number of matters currently before the Queensland courts relating to the importation of cocaine into Queensland. While it would be helpful to detail these matters as a way of showing how cocaine is being imported into the state, given the Terms of Reference of the Commission, regard cannot be had to current judicial proceedings. Accordingly, the Commission is unable to detail these matters any further.

An example of cocaine importation in Queensland that has been recently finalised by the courts is detailed below. While the amounts being imported in this case are much smaller quantities than in other large-scale importations that the Commission is aware of, it provides a useful illustration of how easily cocaine can be imported over a lengthy period of time, through the use of overseas suppliers. The Commission believes the case is an example of an area that organised crime groups will seek to exploit in the future, as Internet-based drug offending gains momentum in Queensland.

### Case study

**R v Verrall**

In *R v Verrall* [2015] QCA 72, the defendant was convicted of one offence of trafficking in cocaine over a one-year period, in addition to a further 14 offences of importing a marketable quantity over two grams of cocaine and one offence of money laundering. The defendant would bring cocaine into Queensland by post and later by courier service. He then sold the cocaine domestically. He arranged for numerous post office boxes to be established in false names with false identification, and he recruited friends and associates to receive packages from couriers in exchange for payment.

The defendant communicated with his supplier in Thailand over a web-based email address. They communicated through the drafts folder in the email in an effort to avoid detection. Packages were intercepted at various points; however, the defendant continued with his importations. At sentencing, a value could not be placed on the amount of money received, because authorities were only able to...
intercept a certain amount of packages, and it was accepted that his business was substantially greater
than what had been found on those occasions.

The Queensland coastline has been identified by the then Crime and Misconduct Commission as a possible
site of exploitation by organised crime groups, who may continue to use small craft to import cocaine.186 One
factor that may limit groups involved in trafficking cocaine is the need to have significant financial resources
and international links to known cocaine source or transit countries.187

However, as demand for cocaine appears to be generally increasing across the state, and the drug is able to
command high prices, the cocaine market will likely remain attractive and lucrative for organised criminal
groups in Queensland.188

UNODC is of the view that a global strategy coordinating supply- and demand-side measures across a range
of countries is required to deal with cocaine.189 It observed that previous prevention and treatment programs
have been successful in promoting the decline in cocaine demand.190 UNODC was also of the view that law
enforcement activities can have a large impact on criminal markets, provided they are applied strategically.191
Without strategic application, law enforcement activities can have perverse effects, such as causing
smaller organised crime groups to emerge where larger ones are dismantled.192 Such repercussions of law
enforcement activities should be monitored and addressed.193

Conclusion

The global cocaine market appears to be relatively stable, with entrenched criminal organisations involved in
producing and trafficking the drug around the world. In Australia, the use of cocaine has increased since the
1990s, and has recently stabilised.

Locally, the drug appears to have increased in popularity. This presents some challenges for law enforcement,
as criminal organisations will continue to involve themselves in a lucrative market—particularly in areas where
cocaine use has been shown to be increasing.

(Endnotes)

The illicit drug market


Addiction. Maryland: Department of Health and Human Services USA, p. 2.


The illicit drug market

References


The illicit drug market

Australian Institute of Health and Welfare, online table 5.16.


The illicit drug market

Queensland Organised Crime Commission of Inquiry


157 R v Power [2013] QCA 351


The illicit drug market

Brisbane: Queensland Government, p. 28


169


170


171


172


173


174


175


176


177


178


179


180


181


182


183


184


185


186


187

3.2.3 Heroin

The drug and its effects on the user

Under Queensland’s Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987, heroin is a prohibited drug, and the unlawful possession, production and supply of, and trafficking in, the drug is a crime.

Heroin (diacetylmorphine or diamorphine) is a highly addictive, semi-synthetic drug. Heroin affects the user by slowing down the central nervous system, reducing the speed that messages travel between the brain and the body. To produce heroin, opium is extracted from the unripe seed pods of opium poppy plants and then filtered to produce morphine. The morphine is then further refined through a chemical process to make heroin base. Heroin may be used in this form; however, it is uncommon in Australia. Usually, the heroin base is further treated with hydrochloric acid to produce a salt.

Heroin has numerous ‘street’ names including Big Harry, boy, black tar, China white, Chinese H, dope, dragon, elephant, gear, H, hammer, harry, horse, junk, low, poison, rocks, skag, slow, smack, whack, white and white dynamite. Heroin is usually injected, but it can also be snorted, smoked, or heated and inhaled as a vapour. It is generally odourless with a bitter taste. It can come in a number of different forms, such as a fine white powder, coarse off-white granules, or as pieces of light brown ‘rock’. In some instances, it may also be on the market as a dark brown tar-like substance, or as a light brown powder. Heroin of this appearance is known as ‘black tar heroin’.

Heroin has numerous ‘street’ names including Big Harry, boy, black tar, China white, Chinese H, dope, dragon, elephant, gear, H, hammer, harry, horse, junk, low, poison, rocks, skag, slow, smack, whack, white and white dynamite. Heroin is usually injected, but it can also be snorted, smoked, or heated and inhaled as a vapour. It is generally odourless with a bitter taste. It can come in a number of different forms, such as a fine white powder, coarse off-white granules, or as pieces of light brown ‘rock’. In some instances, it may also be on the market as a dark brown tar-like substance, or as a light brown powder. Heroin of this appearance is known as ‘black tar heroin’.

Heroin is commonly mixed or ‘cut’ with other substances such as caffeine and methylsulfonylmethane (MSM—a dietary supplement). This makes the drug go further. In addition to being cut with other substances, it is sometimes mixed with cocaine and then injected. Recently, there have been reports of ‘ice’ (a form of methylamphetamine) also being mixed with heroin.

Heroin is sometimes referred to as part of a group of pain-killing drugs called analgesics or opioids. The term opioid usually refers to drugs derived from, or with a similar effect to, opium. Opioids may be naturally occurring, synthetic or semi-synthetic. Other drugs in the opioid family include morphine, codeine, oxycodone, buprenorphine and methadone to name a few. Many opioids are legally available for medicinal purposes at pharmacies, although there is no legal purpose for heroin in Australia.
In some instances, heroin is produced through extraction from opioids such as codeine and morphine. When made this way, it is known as ‘homebake’. However, this type of heroin appears to be less commonly used in Australia than the opium-extracted form.

It is not uncommon for heroin users to turn to pharmaceutical opioids such as morphine or oxycodone medications as substitutes for heroin when supplies of the drug are low or of a poor quality. The opioid methadone is commonly used to replace heroin as part of a treatment program for those dependant on the drug. This kind of treatment is known as ‘pharmacotherapy’.

**Effects of heroin on the user**

Heroin can have a number of adverse consequences on individuals who use or become dependent upon the drug. Despite the relatively low number of heroin users in Queensland and Australia when compared to other drugs such as cannabis, it can have destructive consequences for users due to the addictive nature of heroin, its common use as an intravenous drug, and its effects on the central nervous system. In 2015, the United Nations Office on Drugs and Crime (UNODC) reported that of all the illicit drugs, opioids caused the greatest number of drug-related deaths.

The short-term effects of heroin on a user include a ‘rush’ or intense feeling of pleasure, relief of pain and a sense of relaxation. Heroin can have a number of negative short-term effects on the user such as slurred speech, drowsiness, lethargy, reduced coordination, confusion, dilated pupils, a dry mouth, nausea, vomiting, a reduced appetite, decreased sex drive, constipation, decreased body temperature, decreased blood pressure and lower heart rate. A high dose of heroin may result in difficulty concentrating, falling asleep or passing out, an inability to urinate, itchiness, cold clammy skin, slowed breathing, blue lips and fingers, an irregular heartbeat, or death.

In the long term, heroin can cause damage to the heart, lungs, liver and brain, as well as depression, constipation, irregular menstrual periods and fertility problems in women, decreased sex drive in men, mood swings, and memory impairment.

**Accidental overdose**

The most concerning aspect of heroin use is the possibility of accidental death due to overdose. UNODC estimated that in 2013, there were approximately 187,100 drug-related deaths, with opioids believed to be responsible for the greatest number of these deaths.

In Australia in 2011, there were 208 deaths attributed to accidental overdose on heroin. Of these deaths, 201 occurred in the 15-to-54-year age group. Drugs from the opioid family—including heroin—were responsible for 683 accidental overdose deaths, with 617 of these deaths in the 15-to-54-year age group. Of the opioid deaths in the 15-to-54-year age group, 134 of these occurred in Queensland, which had the third-highest fatality rate behind New South Wales and Victoria, although figures from the Northern Territory and the Australian Capital Territory were not available. Many of these deaths involved the use of multiple drugs, indicating an increased risk of overdose where polydrug use is involved.

Deaths attributable to accidental opioid overdose have increased in recent years, but are lower than in the late 1990s, where opioid overdoses peaked at 927 in 1998, 1116 in 1999, and 938 in 2000. Since that time, there has also been a decrease in the proportion of opioid deaths due to heroin and an increase in the proportion of fatal overdoses due to other opioid drugs.

Opioids are responsible for a large number of deaths because of how they interact with the central nervous system. Opioids slow down the central nervous system, which in turn slows down or even stops a person’s breathing rate. This can cause an increase of carbon dioxide in the blood, which in turn causes organ damage or failure. The risk of death due to respiratory issues is increased when opioids are used with other substances that slow the central nervous system, such as benzodiazepines (tranquilisers), cannabis, and alcohol. Multiple drugs were involved in many of the deaths attributed to heroin or opioids in Australia in
The illicit drug market

Queensland Organised Crime Commission of Inquiry

2011. Use of heroin with drugs such as methamphetamine, amphetamine, or MDMA/’ecstasy’ can place a strain on the heart and kidneys.  

UNODC has also attributed high rates of opioid deaths to the availability and purity of the drugs, as well as to reduced tolerance to the drugs in people who have re-used after a period of abstinence, and to the lack of treatment for opioid dependence.  

In addition to overdoses causing death, heroin and other opioids are regularly responsible for non-fatal overdoses. Globally, studies indicate that between 30 and 83 per cent of opioid and injecting drug users have survived an overdose. In Australia, non-fatal overdose rates for heroin also appear high, with 40 per cent of injecting drug users participating in a recent study reporting overdosing on heroin in their lifetime. Of these, 15 per cent had overdosed in the preceding 12 months. In Queensland, of the participants who responded to overdose queries in that same study, half reported that they had accidently overdosed on heroin in their lifetime. Of these, 16 per cent had overdosed in the preceding 12 months.  

Non-fatal overdoses are also a serious health concern, as they can cause:

- cerebral hypoxia, which is a deprivation of oxygen to the brain that can result in a coma, seizures, brain damage or brain death  
- pulmonary oedema, which is a fluid accumulation in the lungs that can lead to heart failure  
- pneumonia  
- cardiac arrhythmia, which is an irregular heartbeat that may lead to faintness, shortness of breath, dizzy spells or more serious heart problems.  

Surviving an overdose also increases the risk of dying from a later overdose.  

Injecting risks

Heroin can also be associated with a number of other health problems as it is commonly administered through injection. Injection of heroin may cause vein damage, as well as skin, heart and lung infections. Poor needle practices—including sharing needles and not using clean needles—can result in Tetanus, Hepatitis B, Hepatitis C, human immunodeficiency virus (HIV), and acquired immunodeficiency syndrome (AIDS).  

Injecting heroin with dirty injecting equipment can also cause blood poisoning (septicaemia), which can cause skin abscesses and may be fatal. Frequent injections can damage veins and lead to infections of the blood vessels and heart lining and valves.  

On a more positive note, health services including needle and syringe programs in Queensland have decreased heroin-injecting rates and sharing of needles, reducing the incidents of these blood-borne viruses and injection-related harms.  

Dependency and withdrawal

Heroin is highly addictive and can cause withdrawal symptoms in addicts if they are unable to obtain or use heroin, or if they attempt to cease using the drug. Some of these symptoms include cravings, restlessness, irritability, depression, diarrhoea, stomach cramps, leg cramps, restless sleep, yawning, vomiting, decreased appetite, a fast heartbeat, runny nose and goose bumps.  

The addictive nature of heroin can also have adverse social and psychological consequences for users. Heroin dependence causes a user to become preoccupied with the drug. They may continue to use the drug despite the fact that their use may cause or contribute to financial difficulties, relationship problems, employment issues, physical health problems and mental health issues.  

Heroin and pregnancy

Use of heroin and other opioids can affect a pregnant woman by causing miscarriages, premature birth or still births. It may also affect a newborn infant by causing reduced growth, by causing dependency in the womb and subsequent withdrawal symptoms, and by increasing the risk of death from sudden infant death syndrome.
Summary of heroin and health

The impacts of heroin on an individual and their community are numerous and varied. The above is a summary of some of the more well-known, commonly reported impacts, but it is by no means intended as an exhaustive list.

Heroin use, like all other illicit drugs, impacts not only the individual, but can also have devastating effects on a user’s family, friends, spouse, colleagues and the wider community.

The prevalence of heroin

The prevalence of heroin globally

Globally, heroin and opium were estimated to be used by between 12.9 million and 20.4 million people in 2013, equating to approximately 0.4 per cent of the global population. Use was particularly high in Central Asia, Near and Middle East, and Eastern and South-Eastern Europe.

Drugs from the broader opioid family, including heroin, were estimated to be used by between 27.9 million and 37.5 million people in 2013. UNODC estimated that 0.7 per cent of the global population used drugs from the broader opioid family, with North America having the highest number of users.

UNODC appears to limit the term ‘opiates’ to heroin and opium. Opiates, in this sense, are estimated to be less commonly used than cannabis, cocaine, and amphetamine-type stimulants (see chart below). Opiates are also less commonly used than ‘opioids’ but this is unsurprising, as the UNODC considers ‘opiates’ as both their own category, and within the data for opioids.

Estimated global use of illicit drugs 2013 (best estimate)

Since UNODC began estimating illicit drug usage in the late 1990s, the use of opiates (defined by UNODC as consisting of heroin and opium) has remained stable, although changing methodologies may have affected this data. Despite this general stability in the global market, there have recently been reports of an increase in the heroin market in the United States of America.

Although the rates of global use have been stable, the amount of opium poppy being cultivated or grown has increased since 1991. In 2014, the amount of opium being cultivated globally was estimated to be at the highest level since the late 1930s. However, this increase in opium cultivation has not yet been reflected in an increase in heroin supply in most regions. UNODC has estimated that in 2014, the amount of land dedicated worldwide to the illicit cultivation of opium poppy was 310,891 hectares. This is the largest area of land since estimates began in 1998. Although South-East Asia was traditionally the primary grower of opium poppy, in recent years Afghanistan has increased its yield and is now responsible for approximately 85 per cent of the world’s opium. That said, South-East Asia has remained the supplier of the majority of heroin detected in Australia in recent years.
From 2012 to 2013, global seizures of heroin increased by 8 per cent, with seizures exceeding 77 tons in 2013. Although this was an increase from 2012, it is reasonably consistent with the levels of global seizures since 2008.

The prevalence of heroin in Australia

Heroin use in Australia is generally low, and has recently decreased. In 2013, only 0.1 per cent of the country’s population aged 14 years or older reported using the drug in the previous 12 months, which is approximately 20,000 people. This was a decrease from 0.2 per cent of the population—or 40,000 people—reporting recent use of heroin in 2010.

Heroin peaked in popularity in Australia in 1998 with a recent use rate among the population that year of 0.8 per cent. Between 2001 and 2010, recent use of the drug remained stable at 0.2 per cent before dropping in 2013. Lifetime use of the drug has also dropped from 1.4 per cent of the population in 2010 to 1.2 per cent in 2013. It should be noted that Australia experienced a dramatic decrease in the supply of heroin to the country in 2001, largely attributed to law enforcement efforts, among other factors. This could account, in part, for some of the decrease in heroin users since the late 1990s.

Recent use of heroin among the Australian population is reported less frequently than other illicit drugs, reflecting that heroin is not a particularly popular drug in Australia (see table below).

Use of illicit drugs in the past 12 months (% of population)

<table>
<thead>
<tr>
<th></th>
<th>% of Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannabis</td>
<td>10.2</td>
</tr>
<tr>
<td>Ecstasy</td>
<td>2.5</td>
</tr>
<tr>
<td>Meth/Amphetamines</td>
<td>2.1</td>
</tr>
<tr>
<td>Cocaine</td>
<td>2.1</td>
</tr>
<tr>
<td>Halogenics</td>
<td>1.3</td>
</tr>
<tr>
<td>Inhalants</td>
<td>0.8</td>
</tr>
<tr>
<td>Heroin</td>
<td>0.1</td>
</tr>
<tr>
<td>Ketamine</td>
<td>0.3</td>
</tr>
<tr>
<td>GHB</td>
<td>0.1</td>
</tr>
<tr>
<td>Synthetic cannabinoids</td>
<td>1.2</td>
</tr>
<tr>
<td>DANPS (excluding synthetic cannabinoids)</td>
<td>0.4</td>
</tr>
</tbody>
</table>


The heroin market in Australia is mainly concentrated in Sydney and Melbourne, with arrest rates for heroin consumers and suppliers significantly higher in those regions than anywhere else in the country.
Australian heroin users are generally older than other illicit drug users, with a median age in 2013 of 37. This is older than the median ages for cannabis, ecstasy, ‘meth/amphetamines’ (a term used in the 2013 National Drug Strategy Household Survey encompassing both methamphetamine and amphetamine), cocaine, hallucinogens and inhalants. The only drugs with a higher median age than heroin were other pain-killers, analgesics, and misused legal pharmaceuticals. On average, heroin users in 2013 were 10 years older than they were in 2001. This indicates that those who use heroin are ageing, and that there is less up-take from younger members of the population.

Despite the general decrease in heroin use, a concerning trend is becoming apparent in the Australian population in regards to the age at which people between the ages of 14 and 24 years first try heroin. In 2013, the average age of first use of heroin was 16.9 years old. This is a significant decrease from 18.7 years old in 2010. Even at its peak in 1998, the age of first use for this group was higher at 17.6 years old. Lower ages of first use have, however, been recorded in 1995 (16.5 years old) and in 2004 (16.7 years old). The recent decrease is concerning, given the addictive nature of heroin and serious health consequences that can result from heroin use.

Despite its low use in the population, Australians generally perceive heroin as a great concern to the community. Participants in the 2013 National Drug Strategy Household Survey associated heroin with a ‘drug problem’ more commonly than cannabis, ecstasy, ‘meth/amphetamine’ and cocaine. People also associated it with more deaths than other drugs, and among illicit drugs, it was nominated as the second-largest concern for the community behind ‘meth/amphetamines’.

A 2014 study of Australian injecting drug users found that approximately 60 per cent of 898 injecting users had injected heroin in the past six months on a median of 72 days in that period. This equates to approximately 12 days a month of heroin use. Of these, approximately 25 per cent had used it daily.

Nationally, injecting drug users reported that they considered heroin ‘very easy’ or ‘easy’ to obtain. Most users had used a white or off-white powder or rock. Only six per cent of injecting drug users participating in the study had used ‘homebake’ heroin in the past six months.

On an average session, users reported using a median amount of a quarter of a gram of heroin, or one and a half ‘points’. A point is approximately 0.1 grams. In a heavy session, they reported using a median of half a gram, or two and a half ‘points’. Sometimes users buy a ‘cap’ of heroin, which is a small amount that is usually enough for one injection. The median cost of a ‘cap’ of heroin was $50, and the price of a gram of heroin was approximately $320.

In 2013–2014, there were 180 detections of heroin at the Australian border, totalling 118.89 kilograms. Analysis of the heroin determined that in 2013–2014, the heroin primarily originated from South-East Asia. Recently, heroin detected at the border has, for the first time, been found to have originated in South America. Only five homebake heroin laboratories were detected in Australia for the 2013–2014 year, confirming that this type of heroin is not as popular as imported heroin derived from opium plants.

The prevalence of heroin in Queensland

Like Australia, the heroin market in Queensland is reasonably modest. Given its likely small population, it is difficult to ascertain the exact number of heroin users in Queensland. However, the Crime and Corruption Commission (CCC) have recently indicated that heroin is a decreasing market.

The National Drug Strategy Household Survey has estimated that in 2013, less than 0.1 per cent of the Queensland population aged 14 years or older had used heroin in the last 12 months. Arrest rates for heroin and other opioid consumers and providers in Queensland also indicate a small user group, with 318 heroin and opioid arrests in 2013–14. This compares with 20,219 cannabis arrests in Queensland during the same period, and 6,772 arrests related to amphetamine-type stimulants. This indicates that heroin is not particularly prevalent in the community, and is not as commonly used as other drugs. Only hallucinogens and cocaine had lower arrest rates in the state.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Queensland 2013-14 total consumer and provider arrests by drug

<table>
<thead>
<tr>
<th>Drug Type</th>
<th>Queensland Total</th>
<th>Victoria Total</th>
<th>New South Wales Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amphetamine type stimulants</td>
<td>20,219</td>
<td>2,541</td>
<td>2,541</td>
</tr>
<tr>
<td>Cannabis</td>
<td>6,772</td>
<td>677</td>
<td>677</td>
</tr>
<tr>
<td>Heroin and other opioids</td>
<td>242</td>
<td>318</td>
<td>318</td>
</tr>
<tr>
<td>Cocaine</td>
<td>231</td>
<td>231</td>
<td>231</td>
</tr>
<tr>
<td>Hallucinogens</td>
<td>242</td>
<td>242</td>
<td>242</td>
</tr>
<tr>
<td>Steroids</td>
<td>318</td>
<td>318</td>
<td>318</td>
</tr>
</tbody>
</table>


In comparison to the 318 Queensland arrests, New South Wales had 1,113 heroin-related consumer or provider arrests for the same period of time, and Victoria had 1,106 such arrests. Queensland did, however, have higher arrest rates for heroin than South Australia, Western Australia, Tasmania, the Northern Territory and the Australian Capital Territory.

Heroin and other opioids consumer and provider arrests 2013-14

Despite the relatively low user numbers, there are some established heroin markets in Queensland—mainly concentrated in some parts of Brisbane and the Gold Coast.

Injecting drug users in Queensland appear to use heroin less frequently than the national average. A recent study of injecting drug users found that in Queensland, 66 per cent of injecting drug users had used heroin in the six months before the study for a median of 48 days in that period. This compares with the national average of 60 per cent of heroin users that had used the drug in the past six months for a median of 72 days in that period. This was also a decrease from 2013, where 72 per cent of participants in the injecting drug survey reported using heroin in the preceding six months.

Queensland also had lower daily use rates than the national average, with 11 per cent of recent Queensland heroin users reporting daily use. This compares with 25 per cent of national recent heroin users. Daily use in Queensland among recent heroin users is decreasing, with 19 per cent of recent users in 2012, and 18 per cent in 2013, taking heroin daily.
Queensland users were, however, slightly more likely to report that heroin was ‘very easy’ to obtain than national users. 140

Most of the heroin in Queensland originates from South-East Asia, or from Afghanistan in South-West Asia. 141 However, Queensland heroin suppliers generally do not obtain the drug directly from these regions, but instead source it through Sydney and Melbourne. 142 As with the national trend, the cost of heroin in Queensland is reasonably high, with Queensland participants in a study of injecting drug users paying a median of $50 for a ‘cap’ and $400 for a gram. 143 This could in some way account for the lower numbers of users. When considered in light of the data that an average heroin user consumes around a quarter of a gram of heroin per session—or one and a half ‘points’—heroin is clearly an expensive habit.

For example, 66 per cent of people participating in an injecting drug user study had used heroin in the last six months, with median use of 48 days in that period. 144 In Queensland, if they used a quarter of a gram on each occasion, at a cost of $100 per gram, the habit would have cost them around $4,800 in that period. 145 For those who use heroin daily, this would amount to at least $700 a week, although it may be higher, as those users are likely to be more tolerant to the effects of the drug and may need a higher dosage.

In 2012, the then-Crime and Misconduct Commission noted that as heroin users were ageing and there was limited uptake of the drug among younger users, the market was likely to continue to contract in Queensland. 146 Although there is limited reliable data on Queensland heroin use, the national figures indicate such a decline is taking place. The CCC has, however, noted that the heroin market in Queensland should be closely monitored due to a possibility of resurgence and because there is already a market of pharmaceutical misusers in Queensland. 147

The nature and extent of organised crime in the Queensland heroin market

Organised crime plays a role in the heroin market in Queensland and Australia. Because growth of the opium plant is generally restricted to South-West Asia, South-East Asia and Latin America, crime groups tend to be involved in the importation and distribution of the drug rather than in its domestic cultivation or production.

In Queensland, there is no particular organised crime group controlling the market. 151 Those groups that are involved in the heroin market differ from other organised crime groups because they will, at times, coordinate with each other or deal with individuals to facilitate the supply of heroin. The Commission is aware that, in addition to traditional organised crime groups involved in the heroin market, there has, in recent years, been an increase in various ethnic-based groups in the heroin market.

The presence of South-East Asian drug importers, distributors and suppliers in Queensland was examined in a 2013 study. The study adopted the United Nations’ definitions of organised crime and drug trafficking to examine 20 cases of drug offences by South-East Asian defendants in the Queensland Supreme Court. The study particularly examined whether drug trafficking groups, drug distributors and street dealers fell into established organised crime models. 152

The importers were found to operate primarily within a criminal network or core group structure, comprised of individuals that were recruited for specific skills to perform specific tasks. These entities were found to be adaptable and fluid networks with a pool of skills, contacts and knowledge. 153

The study found that the core group comprised a small number of individuals who shared power, making it difficult for them to be detected by law enforcement agencies. 154 These groups are generally unstructured and are surrounded by a larger network of associates. 155

The study found that throughout the cases, there was evidence of people being recruited on the basis of their individual skills, contacts and resources. 156 The cases also indicated that there was importance placed on loyalties and ties between particular individuals and groups. 157

The study found that street dealers tended to be self-governing and that there was not enough information on wholesale distributors to determine a consistent organisational model. 158 On the whole, it was observed that South-East Asian drug trafficking in Queensland is characterised by loosely organised,
The illicit drug market

In recent years, there have been a number of cases before the Supreme Court of Queensland dealing with heroin importation, many related to couriers acting as part of an organised crime syndicate. One such case, now closed, is detailed in the case study below.

Case study

R v Thi Bach Tuyet Do

Do was convicted on a plea of guilty to importing a commercial quantity of heroin. The Supreme Court of Queensland sentenced him to 11 ½ years imprisonment with a non-parole period of seven years and six months.

Do was sentenced on the basis that he was acting as a courier and had brought 3.576 kilograms of heroin in his suitcases on a flight from Vietnam to Brisbane. The total weight of pure heroin was found to be 1.903 kilograms. The wholesale value of the heroin was estimated to be between $600,000 and $1,100,000, with the street value estimated to be between $800,000 and $3,800,000. Do was to receive $20,000 for his role in the enterprise.

Do had previously been convicted in 2002 of importing a marketable quantity of heroin. On that occasion, he was sentenced to eight years imprisonment.

In sentencing Do, Byrne SJA noted that ‘You were an important part of a significant criminal enterprise.’

Defendants such as Do represent an integral cog in the machinery of organised crime groups that recruit couriers to carry out the importation of drugs into Queensland and other states and territories. Couriers such as Do are willing to risk detection and lengthy imprisonment upon conviction, in return for significant financial reward. It is apparent that, in the case of Do, his previous sentence of imprisonment did little to deter him from returning to such criminal activity.

Detective Inspector Mark Slater of the QPS Drug Squad, in an interview with the Commission, noted the following:

...if [they’re] not in custody, then generally you find they’re straight back out doing it again, [they] get a 10-12-14 year custodial sentence for trafficking, [they’re] back out again in four or five and they’re into it again and you [have] a lot of it, there’s new players on the scene but there are a lot of recycled players as well, particularly in the ethnic communities.

This position may change, given that those convicted of trafficking under Queensland’s drug laws are now required to serve a mandatory minimum non-parole period of 80 per cent of the term of imprisonment imposed. Nonetheless, the evidence of Detective Inspector Slater and the case of Do reveal that detection, conviction and lengthy incarceration will not necessarily deter participants in organised crime from continuing with such criminal conduct.

Evidence has been placed before the Commission of a number of heroin trafficking syndicates operating in Queensland in recent years, where investigations have been conducted and charges have been commenced. The Commission is limited by its Terms of Reference and is unable to have regard to or detail these matters.
Conclusion

The use of heroin in Australia is low compared to that of other illicit drugs such as cannabis, ecstasy, cocaine and ‘meth/amphetamines’, and in recent years its use has decreased. Heroin users are generally part of an ageing group and there is less uptake from younger people. However, heroin is a highly addictive drug with many dangerous risks to health associated with its use.

Organised crime plays a role in the heroin market in Queensland, generally by way of importing heroin from Sydney, Melbourne, and overseas, and then distributing the drug locally. Such organised crime groups will, at times, coordinate with each other or deal with individuals to facilitate the supply of heroin. There is evidence of criminal organisations of a particular ethnicity operating in the Queensland heroin market. Participants from those groups have been charged with criminal offences that are currently before the courts and so the Commission is prohibited from having regard to such matters pursuant to its Terms of Reference.

The possession of, production of, and dealing in heroin is appropriately criminalised by Queensland’s dangerous drug laws.

(Endnotes)


The illicit drug market

Queensland Organised Crime Commission of Inquiry
The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry


The illicit drug market


<table>
<thead>
<tr>
<th>Line</th>
<th>Reference</th>
</tr>
</thead>
</table>


3.2.4 MDMA/‘ecstasy’

The drug and its effects on the user

Under Queensland’s Drug Misuse Act 1986 and Drugs Misuse Regulation 1987, MDMA—or 3,4-methylenedioxymethamphetamine—is a prohibited drug, and the unlawful possession, production and supply of, and trafficking in the drug is a crime.

MDMA is the operative drug in what is commonly known as ‘ecstasy’. However, despite many tablets being sold as ‘ecstasy’, the drugs may contain other substances as well as MDMA—or they may not contain any MDMA at all. Some of these substances include caffeine or paracetamol, or illicit drugs such as methamphetamine, other amphetamine-type stimulants, drugs known as piperazines and their derivatives, and drug analogues and new psychoactive substances—including MDPV, mephedrone, drugs from the 2C family, and other drug analogues. In this chapter, the term ‘ecstasy’ may be used to refer to both pure MDMA and to tablets that contain other substances (either in addition to or in substitution for MDMA), which are also passed off as ‘ecstasy’.

3 The illicit drug market

Queensland Organised Crime Commission of Inquiry 103
MDMA is a synthetic drug, which means that it is made by processing chemical ingredients—commonly called ‘precursors’—together to create the substance. Some of the chemicals used to create MDMA include safrole, isosafrole, piperonal, and piperonyl methyl ketone.

MDMA/‘ecstasy’ is typically swallowed but may also be snorted. It can be injected, smoked or inserted into the anus, but these routes of administration are less common. Other names for MDMA/‘ecstasy’ include ‘XTC’, ‘X’, ‘Adam’, ‘beans’, ‘M6M’, ‘ecstasy’, ‘E’, ‘Scooby snacks’, ‘eggs’, ‘essence’, ‘ex’, ‘go’, ‘hug’, ‘lollies’, ‘molly’, ‘pills’, ‘pingers’, ‘roundies’ and the ‘love drug’. Once taken, the effects of the drug can be felt within 20 minutes to an hour, and can last for around six hours.

MDMA is most commonly taken in a pill form; however, it may also come in the form of capsules, crystals or ‘rocks’, and powder. When it presents as a crystal, it often appears as brown sugary rocks, or packaged in capsules. This kind of MDMA has been increasing in popularity recently. Crystal MDMA is absorbed more quickly than tablets or powder, which gives users stronger and longer-lasting effects.

In tablet form, MDMA/‘ecstasy’ is marketed under a number of different logos and brands that are imprinted or stamped onto the tablet. They come in various different sizes, colours and shapes. Recently, MDMA/‘ecstasy’ has been detected in Queensland in the shape of hearts, horse-heads and squares.

Effects of MDMA/‘ecstasy’ on the user

MDMA stimulates the central nervous system, speeding up messages between the brain and the body. It is often referred to as an ‘amphetamine-type stimulant’, along with a number of other drugs, because its chemical structure is similar to amphetamine. However, unlike other stimulant drugs, it also has hallucinogenic effects. Those who take MDMA (or ‘ecstasy’) report feeling happy, euphoric, energetic, close to others, accepting, empathetic, easy going and sensual. Users may also experience a loss of inhibitions, increased confidence, a floating feeling, heightened senses, altered perceptions and hallucinations.

MDMA affects the user because of the way it interacts with chemicals in the brain. The main results are due to an increase in the amount of the neurotransmitter serotonin in the brain. Serotonin plays a role in regulating mood, sleep, pain, appetite, perception, motor activity, cognition, temperature regulation, sexual behaviour and hormone secretion. However, the release of serotonin while on the drug can result in a later depletion of the neurotransmitter, which can negatively affect the user’s mood and behaviour in the days following use of the drug.

The drug also affects the release of other chemicals such as dopamine, noradrenaline and acetylcholine, although it interacts with these neurotransmitters to a lesser extent.

MDMA does not appear to have the same rate of serious health complications as other illicit drugs, such as opioids or methylamphetamine. However, despite generally low levels of serious complications, the drug poses a particular risk to users due to the unpredictable nature of the serious adverse effects when they do occur.

Short-term adverse effects on the user

MDMA can have a number of adverse short-term effects on a user. These include: jaw clenching and teeth grinding, excessive sweating, skin tingles, muscle aches and pains, blurred vision, nausea, reduced appetite, increased heartbeat, increased blood pressure, dehydration, heat stroke, consumption of excessive amounts of water (which may lead to death), irrational behaviour, anxiety, irritability, paranoia and violence, vomiting, high body temperature and seizures.

Once the MDMA/‘ecstasy’ wears off or starts to leave the body, users can experience a ‘come down’ or ‘hang over’. They may suffer from exhaustion, restless sleep, difficulty concentrating, anxiety, irritability and depression.

Deaths caused by the drug

MDMA/‘ecstasy’ use has, in some instances, caused or contributed to a number of deaths. Eighty-two deaths were linked with MDMA use between 2000 and 2005, with 19 deaths attributed to MDMA toxicity alone.
These numbers are significantly lower than deaths attributed to opioids in that period, which amounted to approximately 2,776 deaths for those between 15 and 54 years of age, and slightly lower than the 89 deaths attributed to methamphetamine in that period for those aged between 15 and 54 years. However, it was higher than deaths attributed to cocaine in that period. These figures should be compared with caution though, as different criteria such as the inclusion or exclusion of certain age groups may have been used for the ‘ecstasy’ data.

Deaths linked with MDMA/‘ecstasy’ are sometimes the result of hyperthermia and hyponatraemia. Hyperthermia is where there is an increase in body temperature, which can cause organs to fail. A humid environment such as a rave or nightclub may increase the risk of hyperthermia. In some instances, MDMA/‘ecstasy’ users have died from over-hydration, or hyponatraemia, as too much water can cause swelling of the cells in the brain. People may drink too much water due to physical activity such as dancing, or as an attempt to avoid suffering from hyperthermia.

MDMA—the operative component of the drug known as ‘ecstasy’—may also contribute to deaths through cardiac arrest, stroke and kidney failure. For these reasons, MDMA use by those with a pre-existing condition such as heart disease or circulatory problems may be particularly risky.

Of the 82 cases of death linked to MDMA/‘ecstasy’ use between 2000 and 2005, MDMA/‘ecstasy’ use caused or preceded 67 deaths, yet only 19 were caused by MDMA use alone. This highlights the risk of using multiple drugs at the same time—known as ‘polydrug’ use—which is common among ‘ecstasy’ users. Some of the risks of polydrug use include:

- increased risk of dehydration when used with alcohol
- increased risk of anxiety and reduced brain functioning when used with methamphetamine
- increased strain on the heart and other parts of the body when used with methamphetamine (potentially leading to stroke)
- drowsiness, clumsiness, restlessness and feeling drunk and dizzy when used with antidepressants.

MDMA users may also suffer from adverse effects due to the relatively common practise of mixing MDMA with other ‘fillers’, or substituting other substances completely for MDMA in ‘ecstasy’. Users may not be aware that they have taken a substance other than MDMA that may interfere with either other substances they are using, or that may have their own set of adverse effects. For example, there have been instances where the drug paramethoxyamphetamine (‘PMA’) and paramethoxymepharmphetamine (‘PMMA’) have been found in ‘ecstasy’ tablets. These drugs are particularly dangerous, because they take longer to affect the user than ‘ecstasy’—which can lead to people re-dosing, and, ultimately, overdosing. These drugs have been linked to a number of deaths in Queensland, and are discussed in more detail in the drug analogue and new synthetic drugs section of this report.

Long-term effects of the drug

Limited conclusive information is available on the long-term effects of MDMA/‘ecstasy’. Some studies indicate that it may damage the brain cells that make serotonin, although it is unclear how long these effects may last. There are also indications that users may suffer from cognitive, emotional and memory problems.

Additionally, studies have observed that MDMA/‘ecstasy’ users often have symptoms of depression, but it is unclear if MDMA/‘ecstasy’ causes this depression. There have been some suggestions that MDMA/‘ecstasy’ use may exacerbate depression in those vulnerable to the condition due to personal or family history, stress, or polydrug use.

Caution should be used when interpreting the outcomes of studies on the long-term effects of MDMA/‘ecstasy’ use, because it is difficult to determine the role played by other drugs in their results. Other factors, such as pre-existing psychological problems, also make it difficult to reach definitive conclusions on the role played by MDMA. The frequency of use, period of use, and dosages taken may also affect outcomes—for example, heavy use may be more associated with cognitive impairment than occasional use.

In addition, many studies linking ‘ecstasy’ to adverse psychological effects have been criticised for using poor methodologies.
MDMA/‘ecstasy’ can also contribute to other adverse health effects because it lowers inhibitions. This may lead to an increase in sexual risk-taking behaviours. A 1999 study supported this, finding that there were lower rates of condom use with casual partners when they were intoxicated by MDMA/‘ecstasy’. Those who inject MDMA/‘ecstasy’ may also risk health consequences if they share needles. These risks include contracting HIV or hepatitis infections, suffering from blood poisoning, or having skin abscesses.

Dependency and withdrawal

Unlike a number of other illicit substances, MDMA/‘ecstasy’ has not typically been associated with dependency. Animal studies suggest that although ‘ecstasy’ has some reinforcing qualities, these qualities do not appear to be as strong as in other drugs like cocaine or methylamphetamine. People seeking treatment for their MDMA/‘ecstasy’ use is also uncommon, when considered in light of the high number of MDMA/‘ecstasy’ users. In 2012–2013, there were 331 closed treatment episodes in Queensland for MDMA/‘ecstasy’. In contrast, there were 10,050 closed episodes for cannabis, 1102 closed episodes for heroin in that period, and 3215 for amphetamines. The low numbers for MDMA/‘ecstasy’ are significant, given that it is the second most-commonly used drug in the state. Despite the low numbers, there are some people who report that they have problems controlling their MDMA/‘ecstasy’ use, and who seek treatment accordingly. As such, MDMA/‘ecstasy’ use can become problematic for some users. There is also some evidence to suggest that users can develop a tolerance for the drug, requiring a higher dose to obtain the same effect. This, in turn, can increase some of the risks associated with the drug.

Number of closed treatment episodes for drug use by principal drug of concern, Queensland 2012-13

![Number of closed treatment episodes](image)


Other adverse effects of the drug

In addition to health problems, Australian MDMA/‘ecstasy’ users have reported a number of other adverse effects, which they have attributed to their MDMA/‘ecstasy’ use. In a study conducted by the National Drug and Alcohol Research Centre, 42 per cent of the sample attributed occupational or study problems to their MDMA/‘ecstasy’ use. This was particularly common among women. Work or study problems associated with MDMA/‘ecstasy’ use included trouble concentrating, reduced performance, feeling unmotivated, taking sick leave and not attending class. A minority of participants also reported serious problems such as losing or quitting their job or being unable to find employment.

In the same study, 40 per cent of the sample reported that their MDMA/‘ecstasy’ use had caused relationship problems. These problems included arguments, mistrust, and anxiety within the relationship, but on some occasions they resulted in relationships ending (the user being forced to leave home) or violence.
Approximately 38 per cent of the sample reported that they suffered financial problems due to their MDMA/‘ecstasy’ use. These ranged from not having money to spend on other forms of recreation, to being unable to pay for rent or food.

Those who reported problems associated with their MDMA/‘ecstasy’ use appeared to be heavier—and more regular—users of ‘ecstasy’ and/or other drugs, and to have become involved in drug-taking at an early age.

The prevalence of MDMA/‘ecstasy’

MDMA/‘ecstasy’ became popular as an illicit drug in the late eighties and early nineties, particularly among the dance party, night clubbing, or rave scene. The availability of ‘ecstasy’s’ primary drug component—MDMA—decreased both globally and in Australia from mid-to-late 2008. This is thought to primarily be as a result of improved precursor control globally—particularly in China. However, in more recent years, manufacturers appear to have found either alternative substances to use as precursors, or they have found substances that they can convert into traditional precursors to make MDMA.

Law enforcement agencies have attributed the decrease in MDMA/‘ecstasy’ on the illicit drug market as contributing to the increase in the popularity and development of drug analogues and new psychoactive substances.

‘MDMA/‘ecstasy’ use among the global population is generally low when compared to other illicit drugs. In 2013, it was estimated that between approximately 9.3 million and 28.4 million people worldwide had used the drug in the past 12 months. The best estimate was approximately 0.4 per cent of the population or 18.8 million people. In contrast, MDMA/‘ecstasy’ is one of the most popular illicit drugs in Australia with use well above the global average. In 2013, approximately 2.5 per cent of the Australian population had used MDMA/‘ecstasy’ in the past 12 months. The drug is also popular in Queensland at rates higher than the global average, with approximately 2.4 per cent of the population using MDMA/‘ecstasy’ in the past 12 months in 2013.

This means that the worldwide use of ‘MDMA/‘ecstasy’ is estimated to be similar to the use of cocaine and opiates, but well below the use of cannabis, opioids, other amphetamines, and prescription stimulants.

Estimated per cent of global population using illicit drugs in past 12 months, 2013


MDMA/‘ecstasy’ is particularly popular in Oceania, North America, and Eastern and South-Eastern Europe. Seizure data also indicates that ecstasy is increasing in availability in East and South-East Asia.
The illicit drug market

Despite the general global decline in use, MDMA/ecstasy continues to be popular in certain markets and some regions have seen an increase in popularity of the drug in recent years. In South America, Central America and the Caribbean, MDMA/ecstasy seizures more than tripled between 2008 and 2012, indicating a growing ecstasy market in the region.93 MDMA/ecstasy also reportedly saw a resurgence in Asia in 2012, after years of decline in the region.94 The United Nations Office on Drugs and Crime (UNODC) has noted that some trends may indicate that the MDMA/ecstasy market is recovering.95 One indicator is a return to high levels of MDMA in ecstasy tablets produced in the Netherlands, which is a key source of ecstasy in Europe.96 During the early 2000s, ecstasy coming out of the Netherlands had a MDMA content of 90 per cent.97 In 2009 this dropped to 70 per cent,98 which coincides with a period in which precursors were reportedly more difficult to obtain. By 2011, the average MDMA content of ecstasy pills was back up to 91 per cent.99

Global seizures of the drug also increased in 2012, after a drop in 2011.100 In 2013, global seizures dropped again, although they were not as low as in 2011.101 Although the seizure rates for ecstasy during the period from 2008 to 2013 were significantly lower than previous periods,102 there have been some recent large seizures of ecstasy precursors. In 2011, there were a number of large seizures of safrole and safrole-rich oil in Cambodia, Malaysia, Mexico, Belgium and the United States.103 Similarly, in 2012, large seizures of safrole and safrole-rich oils occurred in Australia and Cambodia,104 and in 2013, seizures of precursors were made in the European Union that would have been capable of producing approximately 170 million ecstasy tablets.105

In East and South-East Asia and Oceania between 2011 and 2012, approximately 66,000 litres of the precursor safrole was seized in the region, which could have been used to produce approximately 44 tons of MDMA/ecstasy.106 UNODC speculated in a 2015 report that this region is becoming an emerging driver of the global ecstasy market, with seizures of the drug higher than in other regions such as the Americas.107

The European Monitoring Centre for Drugs and Drug Addiction in their 2015 report of drug use in the European Union have also noted that the drug appears to be undergoing a resurgence, as evidenced by the recent dismantling of a number of large-scale production facilities in Belgium and the Netherlands.108 The European Union also noted that of the countries that have produced reports since 2012, six had reported a decrease in use, while seven had reported an increase in estimated use.109
It remains to be seen whether recent increases in seizures of MDMA/‘ecstasy’ and its precursors are indicative of a change in the trend of decreasing global ‘ecstasy’ use. In any event, ‘ecstasy’ clearly still holds a market in Europe—even if it is a decreasing one—and the drug is undergoing increasing popularity in Central and South America, as well as a resurgence in Asia.

The prevalence of MDMA/‘ecstasy’ in Australia

MDMA/‘ecstasy’ is one of the most popular illicit drugs in Australia. In 2013, the National Drug Strategy Household Survey indicated that 2.5 per cent of the population—or approximately 500,000 Australians—had used ‘ecstasy’ (which may or may not have contained MDMA) in the past 12 months. Excluding pharmaceuticals, this made ‘ecstasy’ the second-most popular illicit drug in the nation, behind cannabis. The survey also indicated that approximately 10.9 per cent—or 2.1 million people—had tried ‘ecstasy’ in their lifetimes.

Like the global trend, MDMA/‘ecstasy’ use in Australia has been decreasing in recent years. After a steady increase between 1993 and 2007, recent use of the drug dropped in 2010, and continued to decline in 2013.

In Australia, the drug referred to as ‘ecstasy’ was reported in the survey to have been particularly popular among men between the ages of 20 and 29, and it is more likely to be used among those from an average or high socio-economic background than by those from more disadvantaged socio-economic circumstances. This is an interesting trend, as MDMA/‘ecstasy’ is generally not as expensive as some other illicit drugs. However, use among those in the most advantaged socio-economic group decreased at a greater rate between 2010 and 2013 than among the lowest socio-economic group. Those with a middle-range socio-economic status were the only group to increase their use of the drug between 2010 and 2013.

Socio-economic characteristics of recent MDMA/‘ecstasy’ users (% of recent users)

MDMA/‘ecstasy’ use is also more prevalent in major cities than in remote or very remote areas, and the drug is more popular among homosexual and bisexual people, who were 5.8 times more likely to use the drug than heterosexuals.

MDMA/‘ecstasy’ use in Australia is still popular at raves or dance parties, with 63.8 per cent of recent users reporting in the 2013 National Drug Strategy Household Survey that they had used ‘ecstasy’ in that environment. However, people also commonly reported using the drug at public establishments, private parties and in private homes, which could indicate a broader acceptance of the drug in the community, beyond the rave culture.
Australian MDMA/’ecstasy’ users tend to also be younger than users of other illicit drugs. In 2013, the median age of recent ecstasy users was 25 years old. This compared with a median of 30 years for recent cannabis users, 28 years for recent ‘meth/amphetamine’ users, 29 years for recent cocaine users and 37 years for recent heroin users. Only users of hallucinogens had a younger median age.

The age of first use of MDMA/’ecstasy’ in Australia among those between 14 and 24 years old is 18.2 years old. The current age of first use among those aged between 14 and 24 years was younger than the age of first use for most drugs, with the exception of cannabis, heroin, inhalants and illicitly used of pharmaceuticals.

Despite its popularity, those who reported in 2013 as having used ‘ecstasy’ (which may or may not have contained MDMA) in the past 12 months in Australia generally used it on an infrequent basis. The majority of ‘ecstasy’ users responding to the National Drug Strategy Household Survey in 2013 (53.5 per cent) reported using the drug only once or twice a year in 2013, and 32.5 per cent reported use every few months. This is less frequent use than cannabis and ‘meth/amphetamine’ consumption among recent users of those drugs, but more frequent than the use of cocaine among cocaine users.

Although MDMA/’ecstasy’ comes in a number of forms, it appears that in Australia, tablets are the most commonly used form of the substance. A study of the drug use patterns of ‘ecstasy’ and psychostimulant users indicated that in 2014, those users were most likely to take MDMA/’ecstasy’ in its tablet form, and they would usually consume two tablets in a normal session of use. However, other forms of the drug appear to have become more popular recently, with use of the drug in its rock/crystal form increasing significantly between 2013 and 2014.

Part of the popularity of MDMA/’ecstasy’ in Australia may be due to its low cost. The Australian Crime Commission (ACC) reported that in 2013–2014, the prices for one tablet ranged from $15 to $50. The Ecstasy and Related Drugs Reporting System, which studies illicit drug use among a population of ‘ecstasy’ and psychostimulant users, reported that in 2014, the median price paid for MDMA/’ecstasy’ pills nationally was $25, and the median price for a capsule was $30. The median price of powder and crystal or rock MDMA was $250 per gram.

MDMA/’ecstasy’ may also be popular because of its accessibility. In 2014, 89 per cent of those responding to a query on the availability of ‘ecstasy’ to the Ecstasy and Related Drugs Reporting System indicated that they thought it was either ‘easy’ or ‘very easy’ to obtain. According to the National Drug Strategy Household Survey, approximately 7.2 per cent of the population had been offered ‘ecstasy’ or had otherwise had the opportunity to use the drug. ‘Ecstasy’ was more available than cocaine and ‘meth/amphetamines’, but not as readily available as cannabis.
A common trend among MDMA/‘ecstasy’ users is the use of other drugs in conjunction with other substances. According to the Ecstasy and Related Drugs Reporting System, 84 per cent of participants had used other drugs with ‘ecstasy’ on their last occasion of use in 2014. These drugs included not only alcohol and tobacco, but also illicit substances like cannabis, methylamphetamine and cocaine. Despite use decreasing in recent years, MDMA/‘ecstasy’ is still one of the most commonly used drugs among the Australian population.

The Prevalence of MDMA/‘ecstasy’ in Queensland

MDMA/‘ecstasy’ is also one of the most popular drugs in Queensland. In 2013, an estimated 2.4 per cent of the Queensland population had tried ‘ecstasy’, making it the second-most popular of the main illicit drugs behind cannabis, although it is not as commonly used as pain killers for non-medical purposes. Use of the drug in Queensland in 2013 was below the national average, and less common than in most other states and territories.

% of population above 14 years using MDMA/‘ecstasy’ in past 12 months (2013) (Table 7.12 National Drug Strategy Household Survey)

<table>
<thead>
<tr>
<th>State</th>
<th>% of Population above 14 Years Using Ecstasy in Past 12 Months (2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern Territory</td>
<td>0.00%</td>
</tr>
<tr>
<td>Australian Capital Territory</td>
<td>3.00%</td>
</tr>
<tr>
<td>Tasmania</td>
<td>2.00%</td>
</tr>
<tr>
<td>South Australia</td>
<td>1.50%</td>
</tr>
<tr>
<td>Western Australia</td>
<td>1.00%</td>
</tr>
<tr>
<td>Queensland</td>
<td>0.50%</td>
</tr>
<tr>
<td>Victoria</td>
<td>4.00%</td>
</tr>
<tr>
<td>New South Wales</td>
<td>3.50%</td>
</tr>
</tbody>
</table>


In 2012, the then-Crime and Misconduct Commission reported that there had been a contraction of the market for MDMA and similar substances since 2008. This was attributed to the lack of precursor chemicals to make the drug globally. Such a trend is consistent with the National Drug Strategy Household Survey, which shows a decrease in recent use in Queensland from 3.7 per cent in 2007 down to 2.7 per cent in 2010 and 2.4 per cent in 2013. However, the Crime and Corruption Commission (CCC) recently noted that ‘ecstasy’ consumption appears to be returning, and that the drug is of a higher quality than in recent years, indicating a resurgence in the Queensland ecstasy market.

Queensland users also tend to mainly use tablets; however, a recent study on ‘ecstasy’ and psychostimulant users found that there was a decrease in those recently using tablets from 99 per cent in 2013 to 81 per cent in 2014. There was also a significant increase in Queensland ‘ecstasy’ users taking the crystalline or rock form, an observation that has also been made by the CCC. Like national users, ‘ecstasy’ was mainly swallowed, with a small number of users snorting, and around 2 per cent had recently injecting the drug.

‘Ecstasy’ is perceived to be relatively accessible in Queensland, with 81 per cent of Queensland respondents to a study on the drug habits among ‘ecstasy’ and psychostimulant users reporting they found the drug in tablet, capsule or powder form as ‘easy’ or ‘very easy’ to obtain in 2014. MDMA/‘ecstasy’ in its crystal or rock form was also reported by 76 per cent of those responding to the question as ‘easy’ or ‘very easy’ to obtain, but far fewer participants reported on this question.

Consistent with national pricing, the cost of MDMA/‘ecstasy’ in Queensland is reportedly low, with those participating in the Ecstasy and Related Drugs Reporting System indicating a median price of $25 for pills, ranging from as low as $8 to $40.
Queensland MDMA/‘ecstasy’ users also tended to use the drug in conjunction with other substances in 2014. Eighty per cent of respondents to the Ecstasy and Related Drugs Reporting System that had recently used ‘ecstasy’ that year stated that they had also used another substance on the most recent occasion of ‘ecstasy’ use. Most commonly, they reported using ‘ecstasy’ with alcohol, tobacco and cannabis. MDMA/‘ecstasy’ use also appears to be used for events in Queensland. In the period between January 2011 and July 2012, a study was conducted of the quantities of MDMA in wastewater from the Gold Coast. This study indicated that the levels of MDMA in the wastewater gradually increased over this period, with spikes around significant events like New Year’s celebrations and music festivals. However, MDMA use is not just limited to special events, as demonstrated by the Gold Coast area wastewater analysis between July 2012 and December 2014 indicating a significant increase of the estimated daily consumption of MDMA.

The majority of MDMA detected in Queensland is sourced from the southern states; however, before reaching those states, it originates from the Netherlands, Belgium, Poland, Estonia, the Czech Republic, Canada, South-East Asia and West Africa. There have also been some MDMA laboratories located in Queensland in the past, but none were detected in 2013–2014.

The general trend appears to be that MDMA/‘ecstasy’ use is decreasing in Queensland; however, it is still one of the most popular and commonly used illicit drugs. There is also speculation that the market may be returning after a recent decline—although the extent or effect of this supposed resurgence is not yet known.

The nature and extent of organised crime in the Queensland MDMA/‘ecstasy’ market

Given that most of the MDMA/‘ecstasy’ in Queensland originates from the southern states, when considering the presence of organised crime in relation to this particular drug, the Commission has looked at the presence of organised crime in the ‘ecstasy’ market in Australia. Australia has high MDMA/‘ecstasy’ consumption as well as relatively high prices for the drug when compared to other regions. As long as the drug remains popular and profitable, the importation of the drug and its precursors are likely to attract interest from organised crime groups.

South-East Asian organised crime gangs are reportedly involved in high-level MDMA/‘ecstasy’ dealing and importation to Australia. Criminal groups of Middle Eastern descent and outlaw motorcycle gangs are also involved in distributing the drug around the country.

There have also been reports of criminal syndicates in a number of different regions being involved in the importation of the drug or its precursors into Australia. Australian MDMA/‘ecstasy’ or precursor seizures have been linked to groups in Italy, Indonesia, the United Kingdom, Spain, Belgium and the Netherlands. The following case study provides an example of a closed case involving the shipment of MDMA/‘ecstasy’ from Italy to Australia:

**Case study**

**DPP v Barbaro & Anor**

In 2007, a shipment of 3000 large cans of tinned tomatoes was intercepted in Melbourne, the container having been sent to Australia from Italy. It was selected for X-ray examination by customs authorities. Once examined and opened, authorities located 15,193,798 tablets within the tins. The total weight of the tablets was in excess of 4.4 tonnes, and when analysed, these contained in excess of 1.4 tonnes of pure MDMA. If the tablets were sold for a wholesale price of $7/tablet, they would have been valued at approximately $122 million. If the tablets were sold at a street level, the drugs would have been valued at in excess of $400 million. The shipment was addressed to a legitimate company that imported products from Italy; however, alternative contact numbers were given. Those who were to receive the shipment were recorded as acknowledging they would have to repay the money to those who sent the product, estimated to be $10 million AUD. It was noted by the sentencing judge that it was, at the time, the largest amount of ‘ecstasy’ ever seized in the world. It is believed by authorities that the ‘ecstasy’ had been shipped by the Calabrian mafia in Italy to its recipients in Melbourne.
In 2013, the Australian Federal Police (AFP) worked together with the Indonesian National Narcotic Board and the United States Drug Enforcement Administration to dismantle an organised crime syndicate that had the capability to import large amounts of the precursor safole oil into Australia. An Indonesian national was allegedly using the Darknet site Silk Road to distribute approximately 200 litres of safole oil a month around the world, including to Australia. An arrest was made in Jakarta in July 2013, and the production of three safole distilleries was disrupted in East Java.

Also in 2013, after an 18 month investigation, the AFP dismantled an international organised crime syndicate spanning Australia and four European countries. The investigation saw three arrests in Australia, one in the United Kingdom, and search warrants executed in Australia, the United Kingdom, Spain, Belgium and the Netherlands. In Australia, 117 kilograms of MDMA base was seized, which could have been used to manufacture up to 1.37 million ‘ecstasy’ tablets.

In 2012, the then-Crime and Misconduct Commission reported that clandestine laboratories capable of manufacturing MDMA remained low.

The Commission is aware that organised crime groups have been adapting their MDMA/‘ecstasy’-manufacturing strategies to avoid detection by importing substances that do not appear to be precursors themselves, but can later be converted or reconverted into traditional or direct ingredients to make MDMA.

Conclusion

MDMA/‘ecstasy’ remains one of the most popular illicit drugs in Australia and Queensland, despite a recent trend in declining use. Although it appears to have less adverse complications than some other drugs, the severity and unpredictability of those complications, when they do arise, should be cause for concern from the community. Queensland Police and federal law enforcement authorities must continue to work closely with other national bodies to combat organised crime groups further infiltrating the MDMA/‘ecstasy’ industry in Queensland. This is a lucrative market that organised crime groups will seek to exploit, if the availability of the drug and its precursors continues to increase throughout the world.

(Endnotes)


The illicit drug market


3 The illicit drug market


The illicit drug market


The illicit drug market


The illicit drug market


The illicit drug market


3.2.5 Cannabis

The drug and its effects on the user

Under Queensland’s Drug Misuse Act 1986 and Drugs Misuse Regulation 1987, cannabis is a prohibited drug, and the unlawful possession, production and supply of, and trafficking in the drug is a crime.

Cannabis is an illegal drug in most countries, although some jurisdictions, including some Australian jurisdictions, have decriminalised the possession of small quantities for personal use.1

Cannabis comes from the Cannabis sativa plant and has numerous ‘street’ names, depending on the form of cannabis or its method of consumption. Street names include marijuana, hash, hashish, weed, pot, dope, grass, ganja, mull, yarnidi, buddha, skunk, hydro, reefer, joints, buckets, cones and hooch2.

There are approximately 80 different cannabinoids (chemical compounds) within the cannabis plant.3 However, the cannabinoid known as delta-9-tetrahydrocannabinol—or ‘THC’—is considered to be primarily responsible for the psychoactive effects of cannabis on the user.4

Cannabis can be used in the form of a herb, resin, or an oil,5 with the herb being the most commonly used.6 Cannabis herb, often referred to as ‘marijuana’, is a mixture of the dried leaves and flowers of the plant, and is the least potent form of the drug as it has the lowest level of THC.7 Herb cannabis is usually smoked either through a rolled cigarette or through a water pipe (bong).8

Cannabis resin, known as ‘hashish’ or ‘hash’, is made from compressed secretions from the glands of the plant9 and it comes in the form of sheets, balls and blocks.10 It usually has medium levels of THC.11 Resin can be smoked in a pipe or water pipe, mixed with tobacco or herb cannabis and smoked, or cooked with food and eaten.12 When eaten, the effects of THC on the user are delayed, so that they are less intense but longer-lasting.13

Cannabis oil, sometimes called hashish oil or resin oil, is made by extracting THC from the herb or resin with solvent.14 The oil is then applied to either cannabis herb or tobacco and smoked, or it is heated so that the vapour can be inhaled.15 The oil is the most potent form of cannabis, with high levels of THC,16 and have a greater effect on the user.

Cannabis plants are cultivated either outdoors (known as ‘bush’ cannabis), or indoors (using a hydroponic growing set-up). Conditions such as light, temperature, humidity and soil acidity can have an impact on the potency of the plant, which in turn affects the intensity of the drug.17 The United Nations Office on Drugs and Crime (UNODC) has suggested that because ‘bush’ cannabis is subject to the elements, THC levels in this type of cannabis can be inconsistent.18 In contrast, hydroponic cannabis that has been grown in a controlled environment tends to be of a more consistent and higher potency.19 This is supported by anecdotal evidence from cannabis users who report that they can tell the difference between hydroponic and bush cannabis, as hydroponic cannabis generally has stronger effects.20 Despite these reports, a recent study of seized cannabis in New South Wales did not find any significant differences in THC content between bush and hydroponic cannabis.21

In Queensland, the cannabis herb is generally sourced from plants cultivated locally, with some obtained from interstate.22 Both bush and hydroponic types of cannabis are grown in Queensland, as the state has favourable cannabis growing conditions.23 However, hydroponically grown cannabis is the dominant form available in the local market.24 Domestic cultivation and supply of cannabis means it is uncommon for cannabis herb to be imported into the country,25 although resin, seeds and oil are still imported.26 Cannabis oil extraction laboratories have been detected within Australia, with the majority detected in Queensland.27

The Crime and Corruption Commission (CCC) reports that some regional hydroponic cultivation sites or ‘grow houses’ have been linked to interstate crime groups.28 The CCC has also reported that profits produced from cannabis grown in these hydroponic cultivation sites is being used to finance the importation of crystal methylamphetamine or ‘ice’.29
Effects of cannabis on the user

The short-term effects of cannabis on users include a general feeling of wellbeing, a loss of inhibition, spontaneous laughter, talkativeness, a feeling of relaxation, drowsiness, or a quiet and reflective mood. These effects occur due to the cannabinoid compounds in the plant that interact with different receptors in the central nervous system and the immune system.

The common prevalence of cannabis in Queensland and in Australian society may indicate that it is perceived as a relatively ‘harmless’ drug. Although fatal overdoses from cannabis are uncommon due to the low toxicity of the drug, there are still a number of negative short- and long-term effects that cannabis use may have on the health of a user.

Some of the commonly experienced negative short-term effects of cannabis include an increased heart rate, bloodshot eyes, slow reflexes and reaction times, loss of co-ordination, and anxiety. If a person uses cannabis heavily, they may experience hallucinations, vomiting, panic reactions and loss of consciousness. In instances where a person uses a high dose, or is inexperienced in using cannabis, they may also experience some short-term drug-induced psychosis.

Some of the long-term risks of regular cannabis use include an increased risk of developing schizophrenia, a risk of becoming dependent on the drug, an increased risk of developing respiratory diseases, an increased risk of heart attack, and cognitive, memory and learning difficulties.

One of the most concerning aspects of cannabis use is its association with a diagnosis of schizophrenia. Schizophrenia is a mental illness that affects the functioning of the brain, and is characterised by delusions, hallucinations, disordered thoughts and speech, decreased motivation and diminished emotional expression. Symptoms usually develop in adolescence or early adulthood. Schizophrenia affects approximately 1 in 100 people in Australia, and more than 21 million people worldwide. Those who suffer from severe mental illnesses such as schizophrenia have higher rates of mortality and suicide, may be unable to earn a livelihood, and may suffer from interference with their education.

There have been a number of studies that have examined the relationship between the use of cannabis in adolescence, frequency of cannabis use, and the onset of psychotic symptoms and schizophrenia. Many of these studies have found an association between using cannabis on a regular basis at a young age and a diagnosis of schizophrenia. A metadata review of cannabis and psychosis studies in 2004 found that cannabis use appeared to double the risk of later developing schizophrenia. The risk of heavy cannabis users developing schizophrenia remains present, even when other social factors and the use of other drugs are accounted for.

In addition to increasing the risk of developing schizophrenia, some studies have also indicated that schizophrenia is triggered in cannabis users vulnerable to the condition earlier than in other persons suffering psychosis. A 2011 review of 83 different studies found that the onset of psychosis in cannabis users was 2.7 years younger than for non-substance-using control groups.

Cannabis use has also been associated with the exacerbation of symptoms in people already suffering from schizophrenia or another form of psychosis. Cannabis use in those with existing psychotic symptoms can trigger hallucinations, paranoia, and mood swings, and can worsen delusions. People using cannabis while suffering from psychosis are also likely to be less compliant with medical regimes, which can result in poorer health and social outcomes.

It should be noted that although there appears to be an association between cannabis and schizophrenia, no definitive causal link has been proven between the drug and the illness. The Australian Medical Association considers that the most plausible explanation for the association is that cannabis use is one of a number of contributory causes of psychosis in vulnerable individuals.

Despite the lack of a causal link, the association between developing a psychotic disorder and adolescent cannabis use remains concerning, particularly as cannabis is typically the first and, in some instances, the only illicit drug used by adolescents.
The prevalent use of cannabis in some Indigenous communities (discussed later) is particularly concerning in light of the association between schizophrenia and adolescent cannabis use, as Indigenous Australians in more rural and remote communities may have limited access to treatment services. The negative effects of cannabis use on Indigenous communities is reflected in an Australian Institute of Health and Welfare report, which found that between 2006 and 2008, Indigenous Australians were hospitalised for mental and behavioural disorders relating to cannabis use at five times the rate of other Australians. In Queensland in 2011, Indigenous Australians were involved in one in ten cannabis-related treatment episodes.

The use of cannabis has also been linked to depression and anxiety disorders. However, the link between depression and cannabis use is weak, and may be affected by other factors such as family, personality and other drug use. There is also evidence supporting a relationship between cannabis use and anxiety, but it is not sufficient to demonstrate a causal relationship.

Another health concern regarding the use of cannabis is the risk of dependence. The symptoms of substance dependency include: a strong desire or compulsion to take the substance, difficulties controlling consumption of the substance, withdrawal symptoms where use of the substance is stopped, an increased tolerance to the substance, persistence with the substance despite harmful consequences, and neglect of other interests. Although cannabis is less likely to cause dependence than some other illicit drugs, it is estimated that nine per cent of people who use the drug once are at risk of dependence, with that risk rising to one in six if use begins in adolescence. The risk of dependence also increases with regular and heavy use.

Cannabis dependence can negatively affect a number of different areas of an individual’s life, including personal relationships, educational outcomes and employment. Cannabis-dependent persons may also experience withdrawal symptoms such as anxiety, insomnia, depression, and appetite disturbance when not using the drug.

In the past 10 years, there has been an increase in people seeking treatment for cannabis use disorders globally, with cannabis admission treatments increasing between 2003 and 2012 in Western, Central, Eastern and South-Eastern Europe, Latin America and the Caribbean, and Oceania. Cannabis-related treatment in Oceania increased from 30 per cent in 2003 to 46 per cent in 2012.

There has been some speculation that cannabis has increased in THC content and potency in recent years, leading to an increase in both dependence and adverse health effects. Some studies have also indicated lower levels of cannabidiol (a cannabinoid thought to offset the effects of THC) in the drug in recent years. In the United States, there is an increasing trend in cannabis-related treatments from 6.9 per cent in 1993 to 17.5 per cent in 2012. The United Nations Office on Drugs and Crime (UNODC) notes that this coincides with an increase in levels of THC in cannabis from 3.7 per cent in 2007 to 12.6 per cent in 2013.

An explanation for the increase in potency is the increasing prevalence of hydroponic cannabis on the market, which may have stronger THC content since conditions such as light, temperature, soil acidity and humidity can be controlled in an indoor growing environment. However, a study of cannabis seized from New South Wales did not find differences in levels of THC and other cannabinoids between indoor- and outdoor-grown cannabis.

Although UNODC considers that there is a relationship between potency and cannabis dependency, no conclusive link between negative health consequences and increased cannabis potency has been established. Other explanations for the increase in people seeking treatment for cannabis dependency include increased availability of services, court and other criminal justice diversion programs, younger age of first use of cannabis, and differing methods of cannabis consumption.

Regardless of the relationship between potency and dependency, there is clearly a risk of cannabis dependency for some regular cannabis users. This dependency can result in difficulties withdrawing from the drug, and adverse social outcomes.

Respiratory diseases are also a risk of cannabis use in its herbal form, as the smoke contains harmful chemicals. Those who smoke regularly may have a recurrent cough, frequent chest illness, pneumonia, an
increased risk of lung infections, and chronic bronchitis.84 Cannabis smoking, even among users who do not use tobacco, has been associated with acute and chronic bronchitis at a rate comparable to the rates seen in cigarette smokers.85

UNODC reports that the amount of tar in the respiratory tract from cannabis smoke is four times the amount of tar generated from the same amount of tobacco,86 which may have negative implications for the respiratory health of the user.

Although there is evidence of a relationship between heavy cannabis use and chronic bronchitis and poor immunity of the respiratory system, the Australian Medical Association is of the view that this evidence is not conclusive,87 noting that there is variable evidence regarding the relationship between cannabis use and lung cancer.88

Cannabis use may increase the risk of heart attack among those who have previously had cardiovascular problems.89 This is because cannabis use increases the heart rate, which can increase the risk of heart attack—particularly in the hour after cannabis use.90

Some studies have also shown an association between long-term cannabis use and cognitive impairment, particularly in regard to memory, verbal learning, and attention.91 In addition, cannabis users are at risk of adverse effects when they use the drug with other substances. Cannabis is the most commonly used illicit drug taken in conjunction with other substances.92 Use of multiple drugs in combination is known as ‘polydrug use’. Cannabis is often used in conjunction with alcohol, MDMA/‘ecstasy’, methylamphetamine, heroin and cannabimimetics (synthetic cannabinoids).93 In some cases, cannabis is used to relieve the effect of ‘coming down’ off other drugs.94

The mixing of substances increases the risks of harm to the health of cannabis users.95 Polydrug use generally increases the risks of overdose, paranoia, mental health problems, increased heart rate, increased blood pressure and increased body temperature.96 One of the most prevalent combinations of substances is the use of cannabis with alcohol.97 A user mixing these substances may experience heightened nausea, vomiting, anxiety and paranoia.98 It may also increase the risk of psychotic symptoms in vulnerable individuals.99 People using this combination of substances may be less aware of their surroundings and they may engage in risky behaviour such as unsafe sex.100

There has also been speculation that cannabis use creates a risk of harm to the individual as it may lead to the use of or dependency on other harmful illicit drugs. This theory is known as the ‘gateway drug’ theory, and is based on the general pattern of cannabis being the first illicit drug that adolescents try.101 Some studies have shown that the use of cannabis at an early age is associated with the risk of using other drugs, polydrug use, and developing substance abuse problems.102 However, there is no conclusive evidence that cannabis use causes the subsequent use of other illicit drugs.103 and competing theories suggest that personal, social and economic factors may also contribute to the use of cannabis and other illicit drugs.104

In addition to these health-related consequences, heavy cannabis use can also have other social effects on the user. For example, regular and heavy consumption of cannabis may result in the user neglecting their relationships, parenting responsibilities, career, and other personal, social and community priorities and responsibilities.105

Many adverse effects of cannabis are linked with heavy use—or regular use at an early age—and are not necessarily encountered by all or even many cannabis users. Those who use cannabis only occasionally are unlikely to suffer from many of these adverse effects.106 However, it is clear that cannabis use either causes—or contributes to—the risks of suffering from a number of serious health conditions for some users. For these reasons, it is clear that cannabis remains a dangerous drug of concern for the community.

The prevalence of cannabis

Cannabis is the most commonly used illicit drug throughout the world,107 with Australian use of the drug higher than the global average.108 This position is replicated in Queensland, where cannabis is the most popular illicit drug.109
The prevalence of cannabis globally

Cannabis herb is produced in almost every country in the world. Cannabis resin production is more confined, with the majority of production in North Africa, the Middle East, and South-West Asia.

The use of cannabis across the world has been increasing since 2009, although it appears to have decreased between 2011 and 2012. UNODC estimated that in 2013, approximately 181.79 million people globally used cannabis, equating to approximately 3.9 per cent of the global population. This estimate was higher than that of any other drug, with the second most popular type of drug considered to be comprised of amphetamine-type stimulants (which had a significantly lower estimate of 33.90 million users—equating to 0.7 per cent of the global population). Cannabis use is most prevalent in West and Central Africa, North America, Oceania, and Western and Central Europe.

Cannabis is associated with the majority of drug-use offences across the world. In 2014, UNODC reported that the number of people coming into contact with authorities for cannabis use and possession offences increasing by a third in the past decade. However, in some parts of the world—such as Uruguay, Jamaica and parts of the United States—recreational cannabis use is now legal, with regulations around cannabis supply and cultivation.

In the United States, a review of cannabis use in the State of Colorado, conducted after the state changed its laws in 2012, indicates that the prevalence of cannabis there is higher than the national average, with peaks coinciding with the easing of restrictions on personal cannabis consumption. However, there is no causal evidence to link the high usage to the change in legislation. The State of Colorado also had high levels of health treatment admissions concerning cannabis, an increase in calls to poison and drug centres regarding cannabis between 2013 and 2014, and an increase in cannabis detections in people involved in fatal car accidents between 2006 and 2012. In 2014, UNODC speculated that areas legalising cannabis would see an increase in use due to a perception that it is a low risk drug on account of its legality. It also noted that this could make cannabis more attractive for youth and young adults, who are particularly susceptible to some of the health risks associated with the drug. It may, however, be some time before the effects of legalisation are clear.

The prevalence of cannabis in Australia

The global popularity of cannabis is echoed in Australia, with the National Drug Strategy Household Survey indicating that in 2013, one in every three Australians had used cannabis in their lifetime. Further, there was an estimated 1.9 million Australians using cannabis in the 12 months before the survey. Since the survey was conducted, cannabis has consistently been the most popular illicit drug used in Australia, with recent use remaining stable over the past decade.

Nationally, cannabis use is more common among men than women, and is most prevalent in the 20-to-29-year-old age group. Since 2001, the average age that Australians between the ages of 14 and 24 first try cannabis has increased from 15.5 years old to its most recent estimate of 16.7 years old. The previous survey, conducted in 2010, indicated a first use age of 16.2 years. In 1995, the age of first use for the same age group was 16.1 years of age. During the period between 1995 and 2013, the youngest average age of first use was 15.5 years, recorded in 2001. The current age of first cannabis use—16.7 years—is younger than the age of first use for other illicit drugs.
Although popular with younger generations, cannabis has a broad appeal across the Australian population. Use of cannabis by people aged 50 and older is increasing, with these users more likely than younger people to use the drug regularly. The drug also attracts people of different social and economic backgrounds, with almost equal use among people of high and low socioeconomic statuses.

Not only is cannabis the most commonly used illicit drug in Australia, it is also the most frequently used, with those who recently used it reporting that they consumed it at least every few months. Approximately one-third of recent users reported using it on a weekly basis. Those who used cannabis tended to use it more frequently than users of other illicit drugs (such as methylamphetamine, ‘ecstasy’ and cocaine) used those other drugs.

Cannabis is readily obtainable across Australia. In the 2013 National Drug Strategy Household Survey, one in five people aged over 14 years old reported that they had either been offered cannabis or had the opportunity to use cannabis in the 12 months prior to the survey.

The 2013 survey showed that those recently using cannabis overwhelmingly reported using either the head (or flower) of the plant, or the leaves. Cannabis head (or flower) was reportedly used by 72.4 per cent of users, with 44.9 per cent reporting use of the cannabis leaf. In contrast, only 9.8 per cent of recent users reported using cannabis resin, and five per cent recorded using cannabis oil. Participants in the survey were able to nominate more than one form of cannabis used, accounting for the figures exceeding 100 per cent. Use of resin appears to be declining, with 11.5 per cent reporting use of resin in 2007, compared to 9.8 per cent reporting use in 2013.

The popularity of cannabis in its herb form is also reflected in a recent study of the drug habits of ‘ecstasy’ and psychostimulant users, which indicated that use of resin or oil was rarely reported. Similarly, a study of injecting drug users found that on a national level, only seven per cent of participants purchased resin in the six months prior to the interview, and four per cent had purchased hash oil. This is in contrast to the 65 per cent of participants reporting use of hydroponic cannabis, and the 39 per cent that reported use of bush cannabis, in the six months before their participation in the study. Users in that study could nominate more than one type of cannabis used in the past six months, accounting for the numbers exceeding 100 per cent. This pattern of low resin and oil use further indicates that herbal cannabis dominates the Australian market.
The prevalence of cannabis in Queensland

The CCC has assessed the level of risk of cannabis to the Queensland community over the years from 1999 to 2012. While cannabis was given a medium rating in 1999 and 2004, this rating was increased to high in 2009 and continued at high in 2012. It is a drug that is very prevalent within the Queensland community and remains a great concern to law enforcement authorities in this state.

The National Drug Strategy Household Survey in 2013 indicated that 11.1 per cent of Queenslanders aged 14 years or older had used cannabis in the previous 12 months. This compares to 10.2 per cent of people nationally that reported use in the same period. Recent cannabis use was more common in Queensland than in New South Wales, Victoria, South Australia and the Australian Capital Territory.

![Pie chart showing per cent of the population using cannabis in the past 12 months (2013) by state](chart)

Per cent of the population using cannabis in the past 12 months (2013) by state

The popularity of the drug is reflected in its accessibility throughout Queensland. A 2014 study on drug use by ‘ecstasy’ and psychostimulant users indicated that 90 per cent of respondents in Queensland considered hydroponic cannabis ‘very easy’ or ‘easy’ to obtain. Similarly, 84 per cent of Queensland injecting drug users participating in a further 2014 survey reported that hydroponic cannabis was either ‘very easy’ or ‘easy’ to obtain.

Cannabis use in Queensland is most common among people aged between 20 and 29 years old, with people aged 14 to 19 years being the second most likely to have used cannabis in the past 12 months.

Cannabis is reportedly prevalent in Indigenous communities in Queensland, particularly in the far northern regions. This is also reflected nationally, with the National Drug Strategy Household Survey 2013 reporting that recent cannabis use among Aboriginal and Torres Strait Islander people was almost double the rate of recent use among non-Indigenous Australians. It has also been reported that Aboriginal and Torres Strait Islander people are more likely to have first tried cannabis at a younger age, have higher rates of regular use, and are more likely to become dependent on the drug.

The health and social impacts of this high use rate is particularly concerning given that many individuals in these communities face greater health and socioeconomic disadvantage than non-Indigenous Australians. For those living in more remote regions, cannabis is also reportedly significantly more expensive to purchase.

In the past decade, Queensland has been consistently responsible for the greatest proportion of cannabis-related arrests in Australia. This trend continued in the 2013–2014 period, with Queensland accounting for more than 30 per cent of cannabis-related arrests nationally. This was an increase of 10.1 per cent from the 2012–2013 period. Although these figures are an indicator of the prevalence of cannabis in the community, the disparity between Queensland arrest figures and other states could also be due to differing law enforcement practice.
In a 2012 report, the then-Crime and Misconduct Commission noted that far northern policing regions were responsible for the highest number of both cannabis provider and consumer-related arrests between 2007 and 2011. This was followed by northern, north coast, central and southern policing regions. The Crime and Misconduct Commission suggested that the high volume of arrests, particularly in far northern and northern policing regions, may be a reflection of both the popularity of the drug in those areas and the favourable climate and conditions for cannabis cultivation in northern Queensland. These figures could also be due to the national trend of higher use of cannabis by people living in very remote, remote and outer regional areas than people in major cities.

Some of the popularity of cannabis both in Australia and Queensland may be due in part to its affordability. In Queensland, ‘ecstasy’ and psychostimulant users who had recently bought cannabis in 2014 reported that the median price they last paid for hydroponic cannabis was approximately $90 for a quarter-ounce (approximately seven grams), and $280 for an ounce (approximately 28.5 grams). This is on par with the nationally reported median price of $90 for a quarter-ounce of hydroponic cannabis and $300 for an ounce of hydroponic cannabis.

Bush cannabis is slightly cheaper than hydroponic cannabis, with ‘ecstasy’ users who had recently bought bush cannabis in Queensland reporting the median price as $80 for a quarter of an ounce, and approximately $275 for an ounce (with a limited number of people having reported purchasing an ounce). Nationally, the last median price for a quarter ounce of bush cannabis was the same, with the national median cost at $250 for an ounce.

It is difficult to put these prices in context, because how much cannabis herb is used on each occasion may depend on the method used to consume it, the potency of the herb, and the tolerance and preference of the user. A rolled cigarette or joint of cannabis herb has been reported as containing anywhere between 0.25 grams and seven grams of the drug.

Recently, the CCC has noted that there have been anecdotal reports of difficulties in sourcing cannabis in Queensland over the past few months. The CCC have speculated that this may be due to crime groups turning their attention to the supply of ‘ice’ or crystal methylamphetamine.

It is clear that cannabis use is entrenched not only in Queensland society, but across Australia and the world. The popularity of cannabis indicates that there is a high demand for cannabis to be cultivated, produced and supplied. This demand provides opportunities for organised crime groups and entrepreneurial family networks and individuals to involve themselves in—and profit from—the cannabis market.

The impacts of cannabis on society

Cannabis is the most prevalent illicit drug in Queensland and Australia. Although its common use indicates a perception that the drug is ‘harmless’, the use of the drug places social and economic burdens on the state.

One of the main economic impacts that cannabis use has on the community is the burden it places on the health care sector. In Queensland in 2013–2014, cannabis was the principle illicit drug for which treatment related to drug use was sought. It was the principle drug of concern in 34 per cent of drug- and alcohol-related closed treatment episodes (where treatment has ceased for at least 3 months). This is second only to alcohol, which was the principle drug of concern in 37 per cent of closed episodes. In 2010–2011, Queensland drug and alcohol information services also reported that the majority of inquiries they received were about cannabis.

There is limited data available to indicate the economic effect of cannabis use on the health care system. Although some studies have tried to estimate the costs, differing methodologies and the inclusion or exclusion of particular kinds of treatment make it difficult to determine the economic effects with any certainty. While the studies do not specifically address the cost of cannabis use on the health care system in Queensland, they may give some indication of the burden that cannabis use places on the system generally.
A 2007 study estimated that treatment for cannabis dependence and for health consequences relating to cannabis use (including psychotic disorders, traffic accidents and birth problems associated with cannabis use) in New South Wales cost $16,912,123.168

In 2004–2005, the Department of Health and Ageing estimated that $3,054,000 in hospital costs across Australia were attributable to cannabis-related health issues, accounting for 16.4 per cent of gross hospital costs associated with the use of identified illicit drugs, second only to the costs associated with opiate use.169 Cannabis-related health issues accounted for a total of 7,287 days of hospital bed use,170 diverting those beds and services away from people suffering from other medical conditions.

The resulting diversion of services also impacts the Queensland Ambulance Service. The Service reported that it attended to 226 overdose cases where cannabis was the main drug of concern in 2013–2014.171 This is a decrease from the number of attendances in 2012–2013, and on par with the attendances in 2011–2012.172 However, it is an increase in the number of attendances in 2009–2010 and 2010–2011.173 Attendance for cannabis-related overdoses directs ambulance resources away from patients suffering from other health complications.

The criminal justice system is also burdened by cannabis use. Queensland has the highest rate of cannabis-related arrests in Australia. This results in time and costs incurred by police, by the Director of Public Prosecutions, and by Legal Aid Queensland, as well as court costs and, in some cases, corrective services costs.174

A 2011 examination of the cost of cannabis offences to the New South Wales criminal justice system estimated that in 2007, costs related to cannabis enforcement such as policing, court, penalty and other costs were valued at approximately $49,267,123.15. Although this estimate should be treated with some caution due to the limited data available, it provides an overview for some of the economic costs of cannabis enforcement. It should be noted that a cost-benefit study that examined maintaining current drug policy in New South Wales and moving to a legalised system did not show a substantial difference in the cost-benefit between the current system and one in which cannabis is legalised.176

Cannabis use also effects the community socially and economically because it has been linked to poor educational outcomes for those who use it as adolescents, which leads to higher incidents of unemployment and dependence on social welfare.177

There are also safety risks to members of the community who come into contact with an individual under the influence of cannabis. For example, cannabis use may pose occupational health and safety risks, including the risk of injury to both the user and to those around them in a workplace setting. This is due to the reported effects of cannabis on reaction time, information processing, coordination and perception,178 which may impact how a person under the influence of cannabis operates heavy machinery or otherwise performs their duties.

These effects also have implications for the safety of road users. Roadside testing for cannabis and other drugs was introduced in Queensland in 2007 to ‘enhance road safety for the benefit of the entire community’.179 Between 2007 and 2010, two per cent of drivers that were tested by a Roadside Drug Testing Unit tested positive for cannabis.180 In some areas, drivers tested positive for cannabis at higher rates than they did for alcohol.180 The Deputy Commissioner of the Queensland Police Service (QPS) has advised in a sworn statement to the Commission that in the period 1 July 2014–30 June 2015, QPS conducted 20,839 tests under the roadside drug testing program. Of those tests, 910 tested positive for the presence of cannabis. These numbers are concerning, because a number of studies have made an association between cannabis use and risk of crash involvement;182 with some indicating that cannabis use may increase the risk of crashes by two to three times.183

Other safety risks associated with cannabis include the risks posed by hydroponic grow houses. These houses may expose residents, neighbours, landlords and professionals such as police officers to health risks from chemical and contaminant exposure and fire risks from poor electrical set-ups.184
The nature and extent of organised crime and the cannabis market within Queensland

There is an organised crime presence in the Queensland cannabis market. Organised crime groups are involved in the production and distribution of cannabis in the state, either through cultivating crops of bush or hydroponic cannabis locally, or transporting cannabis into Queensland from other states—mostly South Australia and Victoria.\(^{185}\)

In an interview with the Commission, Detective Inspector Mark Slater of the QPS Drug Squad advised that while hydroponic cannabis cultivation does occur in Queensland, the majority of Queensland-grown cannabis is bush cannabis. Detective Inspector Slater went on to note that much of the hydroponically grown cannabis in the Queensland market comes from interstate, particularly South Australia and Victoria. That cannabis arrives in Queensland through a number of mechanisms, including by car, other transport vehicles and, in some instances, commercial aircraft.\(^{186}\) The CCC has noted that the courier, freight and trucking industry continue to transport cannabis from interstate to Queensland, and that the level and sophistication of concealment methods has been increasing.\(^{187}\)

The Queensland cannabis market is not controlled by one particular crime group. Rather, due to high demand and profitability, the market attracts a diverse range of participants.\(^{188}\) Cannabis production and supply holds an appeal to organised crime groups because it is a reliable and consistent source of income, with a low risk of detection by law enforcement agencies.\(^{189}\)

Family networks and generational operations are particularly dominant in the Queensland cannabis market,\(^{190}\) with a number of QPS operations involving family-orientated cultivation. A number of the most recent examples of these types of cannabis crops grown and trafficked through family operations are either the subject of ongoing investigations or subject to current court proceedings. As a result, this Commission cannot discuss these matters; the Terms of Reference prohibit the reporting of current proceedings. However, detailed below is an example of a closed case involving a family that produced and distributed cannabis on a very large scale throughout Queensland. The court recently dealt with the final member of this family who was charged in relation to this matter.

---

**Case study**

**The Gardner Family**

The father of the family, Michael Gardner Senior, was sentenced by the Supreme Court of Queensland in 2012, with his appeal being finalised later that year.\(^{191}\) Numerous members of his family have been dealt with in the Supreme Court and Court of Appeal in relation to this operation, with the most recent member, the son, having his court proceedings finalised this year.\(^{192}\) The father, dealt with as the principal offender, was convicted for trafficking in cannabis, and received a sentence of 13 years’ imprisonment. The trafficking was alleged to have occurred over a four-and-a-half-year period. He was sentenced on the basis that he was the central figure in a large-scale trafficking operation involving the production, packaging and distribution of cannabis.

The production took place on a large, remote property in Southern Queensland that had been purchased for the sole purpose of producing cannabis. The front 2,000 acres of the property was grazing land, which could be used to mask the illegal production occurring at the back of the property. When police executed a warrant on the property, they located eight different cannabis fields of various sizes, with the largest measuring 30 metres in width by 300 metres in length. Cannabis had been grown and harvested from all but one of those sites, which still had half the crop left. That remaining crop alone comprised 22,000 plants. A sample of 100 of those plants was weighed with roots removed, totalling 51.9 kilograms. There were numerous drying sheds and tents on the property which contained cannabis which had been harvested. The total weight of the usable cannabis in the drying sheds alone was 3.59 tonnes.
The approximate value on the black market for the cannabis was $68.95 million. That value would increase when one considers it being sold further down the chain of users. Those figures did not take into account a further sale—which occurred at the direction of the defendant whilst on remand—or the earlier harvests which no doubt were significant, considering the quantity of cannabis remaining in half of one field.

There were three different campsites on the property with high towers. This would indicate that people were living on the property to tend to and protect the crop. There was machinery located to assist in the production and harvesting of the cannabis. The crops were watered by sprinkler systems fed by industrial water pumps, seven of which were located. The water was fed through approximately eight kilometres of piping to reach the crops. There were also a large number of weapons located on the property. The evidence was that over the years, the father would use cash to purchase items to be used in the production, often used aliases, was known to wear disguises and was, overall, very secretive in his conduct.

Of concern was the way in which the father used his children and step-children—both adult and juvenile—to assist in his production. There was evidence that he had used his step-children, who were at the time aged 11, 12 and 13, to assist in the production. He also used his three adult children in the production.

By the time of his trial five family members gave statements against him. The young children, in their statements to the police, recalled occasions where they were required to hide large amounts of money in their shoes while in a motor vehicle to avoid detection by police, as well as participating in the planting of a large cannabis crop. In the appeal of one of the adult children, it was noted by the court that the father had taught the children to maintain the cannabis plants, distinguish male plants and to weed.

The members of the family were dealt with by the Supreme Court in a more lenient way than the father, given their role in the offences, their co-operation by providing statements against the father, and the fact that they were acting under the direction of the father, who was the dominant person in both the family and in the drug operation. A number of family members received a reduction in sentence pursuant to section 13A of the Penalties and Sentences Act 1992 (Cooperation with law enforcement authorities to be taken into account – undertaking to cooperate).

Kelly Millard was married to the principal between 1999 and 2006. Her three children were the juveniles referred to earlier. Millard pleaded guilty to one offence of producing a dangerous drug and was sentenced to three years’ imprisonment, wholly suspended for an operational period of five years. Her sentence was reduced in accordance with section 13A of the Penalties and Sentences Act.

AM (the stepdaughter of the father) was sentenced for her role in the last production in 2007. She was 17 years old at the time of her sentence in the Brisbane Magistrates Court and received a 12 month good behaviour bond. Her sentence was reduced in accordance with section 13A of the Penalties and Sentences Act. She was not prosecuted for her conduct as a child.

Michael Gardner Junior (the son of the father who worked at the property at different times) pleaded guilty to a number of offences concerning the drug operation, including one offence of producing a dangerous drug. He was sentenced to five years’ imprisonment, suspended after serving 12 months for an operational period of five years. His sentence was reduced in accordance with section 13A of the Penalties and Sentences Act.

Rosemary Gardner (the daughter of the father and who worked at the property over two distinct periods of production) was sentenced to four years’ imprisonment, wholly suspended for an operational period of five years. Her sentence was reduced in accordance with section 13A of the Penalties and Sentences Act.

Kristen Gardner (the son of the father who worked at the property over two distinct periods) was convicted on a plea of guilty to two offences of producing a dangerous drug. He received an effective sentence of five years’ imprisonment, with a recommendation for release on parole after serving 15 months. That sentence was not disturbed on appeal.
This case study reveals the potential magnitude of cannabis cultivation and the ability to generate enormous profits. The numbers outlined in the case were based only on the cannabis that was actually recovered. There is no doubt that there would have been significant quantities involved throughout the entire production, taking into account the cannabis that had already been harvested and sold. This family is only one example of a cannabis production operating in Queensland; other productions by organised criminal enterprises have and continue to occur.

In addition to local family networks, there is some evidence of transnational organised crime in the Queensland cannabis market. The CCC has reported instances of cannabis being imported from Papua New Guinea into Queensland through the Torres Strait, such as in the example of the closed case below.

**Case study**

*R v Neliman*

Neliman was sentenced in the Supreme Court of Queensland at Cairns on 25 February 2013, after pleading guilty to four counts of importing cannabis, one count of trafficking in cannabis and one count of possessing ephedrine. Neliman was a resident of the Torres Strait. He was implicated in criminal conduct through the use of telephone intercepts.

Intercepts recorded conversations Neliman had with others in Papua New Guinea, where he was offering to exchange cash and firearms for 50 kilograms of cannabis. The authorities intercepted him on a beach near Bamaga, in possession of over nine kilograms of cannabis and a small amount of ephedrine. In a police interview, Neliman admitted to importing cannabis into Australia from Papua New Guinea on four occasions. He would travel by dinghy and exchange money and firearms for drugs. He would then bring the drugs back to Queensland and sell them in small quantities.

The sentencing judge noted that, while detecting the importation of drugs is difficult, in that part of Australia it is particularly difficult. This is due to the regularity of travel between Papua New Guinea and Queensland by small boats, and the fact that these boats are not entering through main entry points and are, therefore, not subject to the same risks of detection. The sentencing judge did comment that ‘it is not a case involving major gangland penetration with imported drugs into some sort of network of distribution in mainland Australia.’ Neliman was sentenced to four and a half years’ imprisonment with an early parole release date.

While Neliman was not connected to any organised group within Queensland, the case is an example of a geographical area of concern where cannabis is being imported into the State with limited likelihood of detection.

Organised crime groups may also be involved in the production of cannabis oil. In 2013–2014, five cannabis oil laboratories were detected in Queensland, with only two other laboratories detected nationally during that time. None were detected in Queensland during the 2011–2012 and 2012–2013 financial years, indicating that crime groups may be expanding into this emerging area of the Queensland cannabis market.

A concerning aspect of the Queensland cannabis market is the frequency with which weapons are seized in conjunction with the production and supply of cannabis. The presence of weapons in such circumstances indicates that there is a level of violence, intimidation and sophistication involved in the cannabis market.

In addition to the recruitment and involvement of family members in the production of cannabis in Queensland, the authorities have information indicating that industry professionals are also being used by crime groups to assist in their cannabis production operations. These professionals include:

- mortgage brokers and real estate agents who assist in locating ideal property locations for cannabis cultivation
The illicit drug market

Queensland Organised Crime Commission of Inquiry

- builders and tradespeople who modify homes to accommodate hydroponic cannabis crops
- freight, courier and other transport operators who transport cannabis into Queensland from interstate.202

Detective Inspector Slater of the QPS Drug Squad, in his interview with the Commission, noted that while there is information to suggest that these practices are occurring, this has not been an area where the QPS has targeted and charged people. Indeed, the information provided to the Commission has failed to identify particular instances of charges being laid against facilitators such as mortgage brokers and real estate agents in relation to these types of practices. This suggests to the Commission that in Queensland, there is a lack of evidence that any such conduct engaged in by professionals is done so knowingly.

Nationally, the Australian Crime Commission reports that low- to medium-level criminal networks capitalise on the cannabis market’s profitability and strength, and are well-established in the market.203 There are also reports, dated in 2008, of an increasing involvement in cannabis distribution in Australia by South-East Asian crime groups.204

The pattern of domestic crime groups supplying the cannabis market is reflected in seizures made by the Australian Customs and Border Protection Service. In 2013–2014, it made approximately 2,840 detections of cannabis that cumulatively weighed approximately 158 kilograms.205 This was a decrease in the number of detections from the 2012–2013 year, but an increase of 635.3 per cent in total weight of detected cannabis.206 Cannabis seeds accounted for 95.2 per cent of these seizures.207 Cannabis was most commonly detected in international mail, rather than air or sea cargo or on flight passengers or crew. However, sea cargo was responsible for the greatest weight of seizures.208

The ease with which cannabis seeds can be ordered anonymously online—and the relatively low risk of detection of these parcels due to the high volume of international mail—is an incentive for organised crime groups to involve themselves in cultivating, producing and supplying cannabis.209

One of the main difficulties for law enforcement in disrupting organised crime groups involved in the cannabis market is the inability to easily detect cannabis crops. This is particularly the case as the market increasingly embraces hydroponic technology, which conceals crops indoors and in increasingly urban settings.210

Instances of people charged with production of hydroponically grown cannabis regularly come before the Queensland courts. It is not uncommon to see cases where houses are devoted entirely to indoor plantations. Earlier this year, the QPS charged a large group of people with various drug offences associated with the production of cannabis by using a house for this purpose. Because this matter is still before the courts, the Commission is unable to detail the matter further. However, this type of production is not uncommon in Queensland, and is an area of increasing concern for the State.

While the market remains popular and profitable, and the risk of detection for producing cannabis or importing cannabis seeds remains low, family networks and other organised crime groups are likely to continue to maintain a strong presence in the Queensland cannabis market.

Conclusion

Cannabis use is prevalent throughout Queensland, Australia, and the world. The popularity of the drug indicates a general perception that the drug is relatively harmless. Although not associated with fatal overdoses and dependence to the same degree as other drugs, its heavy use is associated with a number of adverse health consequences, which ultimately cost the economy and community more generally. The QPS has noted that “[t]he increasing societal perception of acceptance of cannabis use and/or increased level of tolerance in the community has seen cannabis considered to be a soft drug irrespective of the harms associated with its misuse.”211 Given the prevalence of cannabis use within the community and the degree of harm associated with such use, the possession of and dealing in cannabis is appropriately criminalised by Queensland’s dangerous drugs laws.
Organised criminal groups are clearly in existence within the Queensland cannabis market. Family groups as well as other organised groups play a large role in the market. It has been established that the potential for financial gain is great, particularly in instances where large-scale productions take place. Detecting these large-scale productions can present difficulties for law enforcement, given the increasing prevalence of these establishments on large properties, which often have the façade of a legitimate farming property due to the large size and location of the land. Further, the increasing production of hydroponic cannabis is of concern.

Where there is demand and profitability in an illicit market, there is an attraction for organised crime groups to gain and maintain a foothold. This has proved to be the case with cannabis in Queensland, where family networks and other groups take advantage of the popularity of the drug and the low likelihood of detection. The QPS has been focused on this drug as a drug of concern to the Queensland community through the National Drug Strategy.

It is the view of the Commission that cannabis should remain of great concern to the community and a drug of focus for the law enforcement agencies in this state.

(Endnotes)


The illicit drug market


The illicit drug market


3 The illicit drug market


The illicit drug market

queensland organise crime commission of inquiry

3

The illicit drug market

141
The illicit drug market


The illicit drug market

Queensland Organised Crime Commission of Inquiry


Transcript of Interview, Mark Slater, 1 July 2015.


R v Gardner (Senior) [2012] QCA 290.


Supreme Court Sentence before Byrne SJA, 26 May 2011.

Supreme Court Sentence before Philippides J, 8 December 2011.

Supreme Court Sentence before Atkinson J, 5 September 2013.


R v Neliman, Supreme Court of Queensland, 25/2/13.

R v Neliman, Supreme Court of Queensland, 25/2/13.
3.2.6 Drug analogues and new psychoactive substances

The drugs and substances and effects on the user

Drug analogues are synthetically created substances that have a similar chemical structure to another drug and/or have a similar pharmacological effect as the other drug. A substance that is similar in chemical structure is a structural analogue. A functional analogue is a compound that has similar pharmacological properties to another drug. Some substances are both structural and functional analogues, because they are similar in chemical structure and pharmacological effect to another substance.

The term ‘new psychoactive substances’ refers to synthetically created substances designed to mimic a prohibited drug (in effect, functional analogues). The term ‘new’ does not necessarily mean that the substances are newly discovered, as some of these compounds have been known to researchers for decades. Rather, the reference to ‘new psychoactive substances’ refers to their new use on the illicit drug market.

For ease of reading, the term ‘drug analogue’ is used in this chapter, and includes new psychoactive substances.

Drug analogues are often advertised as legal alternatives to traditional illicit drugs such as heroin, MDMA/’ecstasy’, cannabis, LSD and amphetamines. They have been increasing in global popularity since the mid-2000s.

Although illegal in Queensland, drug analogues are accessible over the Internet and have recently been available over the counter at adult stores, drug paraphernalia stores and ‘legal high’ stores. Drug analogues can come in a number of different forms, including as pills, powders, sprays, tabs and smoking material.
are sold online and in stores under brand names, but are often labelled as ‘bath salts’, ‘plant food’, ‘research chemicals’, ‘incense’ and ‘herbal blends’ to avoid detection from customs and law enforcement agencies.

The growth in popularity of synthetic drugs is, in part, due to attempts to circumvent drug regulations. Around the world, the method for prohibiting the production, supply, possession and importation of particular drugs is usually by identifying and listing the substances in legislation regulating drug use.

This method of prohibition is easily exploited by producers of drug analogues. When a synthetic drug is discovered by authorities and added to the legislation as an illegal drug, those producing the drug alter its chemical structure. This creates a new substance with a similar effect that is not an ‘illegal’ drug under the legislation, because it has a different chemical composition to the listed prohibited drug.

Queensland’s Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987 criminalise the possession of, and supplying of, dangerous drugs. The Drugs Misuse Act defines the term ‘dangerous drug’ to include a substance specified in schedules 1 or 2 of the Drugs Misuse Regulation. Prior to 2008, the synthetic drug market was able to exploit the law. However, in 2008, the definition of ‘dangerous drug’ was extended to apply to drug analogues and new psychoactive substances. The Drugs Misuse Amendment Act 2008 amended the definition to also apply to substances with a substantially similar chemical structure and substantially similar pharmacological effect as a scheduled dangerous drug.

However, proving that a substance is both similar in its chemical structure and in its pharmacological effect presented evidentiary difficulties for the Crown, and in 2013 the definition was amended to provide that the Crown need only prove one of the limbs, that is, need only prove that either the substance is structurally similar or has a similar pharmacological effect. Further, the definition was extended to apply to a substance intended to have a substantially similar pharmacological effect to a scheduled dangerous drug. It is now illegal to traffic, produce, supply or possess any substances that have either:

- a substantially similar chemical structure to a scheduled dangerous drug; or
- a substantially similar pharmacological effect to a scheduled dangerous drug; or
- a substantially similar intended pharmacological effect to a scheduled dangerous drug.

The Commission understands that, despite the extended definition of ‘dangerous drug’, it can still be difficult for the Crown to prove that a substance is a drug analogue—that is, to prove to the requisite standard of proof, the substantially similar chemical structure or substantially similar pharmacological effect. In particular, proving the latter element is problematic when dealing with a new substance that is yet to be tested.

In response to a Notice issued by the Commission, Mr Michael Walsh, Director-General of Queensland Health, advised that Queensland Health’s forensic chemists experience difficulties in preparing evidence to satisfy the definition. Mr Walsh advised that the difficulties relate to the phrase ‘substantially similar’, a term that is not defined in the legislation. The lack of definition renders the phrase ‘vague and open to interpretation and challenge’. When dealing with a novel substance, forensic chemists will provide additional opinion evidence outlining how the new substance could be said to be substantially similar in chemical structure to an existing scheduled dangerous drug. Satisfying the court that a novel substance is substantially similar in its pharmacological effect has been problematic. As Mr Walsh stated:

[it] is not possible to know or discover the full complex pharmacology of a position in a person that has never been tested and will never meet the standards required for human testing to ever be considered.

The Commission also sought information from the Office of the Director of Public Prosecutions (ODPP) and the Queensland Police Service (QPS) to determine the success of prosecutions for producing drug analogues or new psychoactive substances. While the records kept by the ODPP do not differentiate between different drugs, the QPS was able to advise of nine prosecutions commenced in relation to such substances. Of these prosecutions, only one has resulted in a conviction. One matter remains before the courts, but the other seven defendants either had these charges discontinued or were acquitted. Detective Inspector Mark Slater of the QPS Drug Squad, in an interview with the Commission, spoke about the difficulties. He confirmed that,
apart from their chemical diversion desk, the police service does not have specific police officers tasked with investigating the emergence of these new drug analogues on the market.\textsuperscript{12}

The evidence before the Commission suggests that the extended definition of dangerous drug in the Drugs Misuse Act is causing evidentiary difficulties for the prosecution. The term ‘substantially similar’ lacks definition, and the extended definition is difficult to satisfy in the case of novel substances. In his response to the Commission, Director-General of Queensland Health, Mr Michael Walsh, noted that a number of other jurisdictions use the term ‘analogue’ and include a set of chemical definitions as an alternative to using the ‘substantially similar’ approach. Mr Walsh concedes that this alternate approach has met with issues of its own.

It is the Commission’s view that the extended definition of the term ‘dangerous drug’ within the Drugs Misuse Act—that is, limb (c) (i), (ii), and (iii)—should be reviewed to determine whether the definition effectively facilitates the successful prosecution of the unlawful possession of, and dealing in, drug analogues. In particular, such review should examine alternative approaches in other jurisdictions. As an aside, the Commission notes limb (c)(iii), which extends the definition to a substance intended to have a substantially similar pharmacological effect to a scheduled dangerous drug. The Commission queries the utility of this limb, which would appear extremely difficult to prove.

**Recommendation**

3.2 The Commission recommends that the Queensland Government review the extended definition of the term ‘dangerous drug’ within the Drugs Misuse Act 1986—that is, limb (c) (i), (ii), and (iii)—to determine whether the definition effectively facilitates the successful prosecution of the unlawful possession of, and dealing in, drug analogues. In particular, such a review should examine alternative approaches in other jurisdictions.

The extended definition of dangerous drugs in the Drugs Misuse Act is clearly used as a ‘stop gap’ with new drug analogues specifically included in the schedules once identified.

The drug analogues commonly available in Queensland can be categorised into three main types: cannabimimetics, stimulants, and hallucinogens.\textsuperscript{13}

**Cannabimimetics**

Cannabimimetics—sometimes called synthetic cannabis or synthetic cannabinoids—mimic the effects of cannabis on the user. They do this by replicating the effect of chemical compounds contained in the Cannabis sativa plant, called cannabinoids, on receptors in the body. In particular, they replicate the effect of the compound delta-9 tetrahydrocannabinol (THC), which is primarily responsible for the psychoactive effects of cannabis on the user.\textsuperscript{14}

Cannabimimetics were originally produced for research purposes,\textsuperscript{15} but appeared on the global illicit drug market around 2004.\textsuperscript{16} The most widespread synthetic cannabinoid is the compound known as ‘JWH-018’.\textsuperscript{17} This substance is thought to be approximately three times more potent than the THC found in the cannabis plant.\textsuperscript{18}


Cannabimimetics usually come in the form of inactive plant material that has been sprayed with a synthetic formula to give it psychoactive effects.\textsuperscript{20} This material is then smoked or consumed as a tea.\textsuperscript{21} Cannabimimetics have also been known to come in a powder,\textsuperscript{22} pills and tabs.\textsuperscript{23} In Europe, liquid cannabimimetics have recently appeared on the market for use with electronic cigarettes.\textsuperscript{24}
There are currently 42 cannabimimetics listed in Schedule 2 of the Drugs Misuse Regulation.25

**Stimulants**

Stimulant drug analogues are drugs that mimic the effects of stimulant drugs such as amphetamines, ecstasy and cocaine. There are a number of different types of stimulants that have been detected in Queensland. Some of the commonly known stimulant drug analogues include:

- 4-methylmethcathinone, which is also known as mephedrone
- 3,4-methylenedioxypyrovalerone or MDPV
- Paramethoxyamphetamine or PMA and paramethoxymephamphetamine or PMMA
- Alpha-pyrrolidinovalerophenone or Alpha-PVP.26

The analogue 4-methylmethcathinone (commonly known as Mephedrone, but also known as 4-MEC and 4-MMC)27 stimulates the central nervous system and is used as an alternative to amphetamines, MDMA/‘ecstasy’ and cocaine.28 Mephedrone is often referred to as a ‘synthetic cathinone’, because it has a chemical structure similar to the structure of ‘cathinone’, a compound found in the khat plant.29

Users of mephedrone may experience a sense of euphoria, energy, talkativeness, and hallucinations.30 It is often sold as pills, capsules or as a white or light coloured powder or salt.31 Mephedrone is typically swallowed, although the powder may be sniffed or snorted.32 There are also reports that some users inject the drug.33 It is commonly marketed on the Internet as ‘bath salts’, ‘plant feeder’ and ‘research chemicals’.34

The analogue 4-methylmethcathinone, or mephedrone as it is commonly known, is classified in the Drugs Misuse Regulation as a Schedule 2 dangerous drug.

MDPV is another drug of the synthetic cathinone family that has been detected in Queensland.35 MDPV is a central nervous system stimulant.36 The effects of MDPV are similar to cocaine and methamphetamine, with the exception that MDPV is more potent and longer-lasting.37 Although the substance or compound was first synthesized in the 1960s, it was first reported on the illicit drug market in 2007.38 The analogue 4-methylenedioxypyrovalerone, or MDPV as it is commonly known, is classified in the Drugs Misuse Regulation as a Schedule 2 dangerous drug.

MDPV is commonly sold as ‘bath salts’ under brand names such as ‘Ivory Wave’ and ‘Vanilla Sky’.39 It comes in the form of a powder, pills or capsules,40 and is consumed through smoking, snorting, swallowing, rectal administration or injection.41

PMA and PMMA are stimulants also present in Queensland.42 They are chemically classed in a group of substances called phenethylamines.43 PMA is said to have an amphetamine-type effect, while PMMA has effects similar to MDMA/‘ecstasy’.44 PMA and PMMA are often combined and passed off to consumers as ‘ecstasy’.45 Paramethoxyamphetamine (PMA) and paramethoxymephamphetamine (PMMA) are classified in the Drugs Misuse Regulation as a Schedule 1 dangerous drug.

PMA and PMMA are not particularly ‘new’ substances. PMA has been available in the United States and Canada since the 1970s.46 After the drug emerged on the market in the 1970s, it was linked with a number of deaths, and as such it did not become popular on the illicit drug scene.47 Recently, however, the drug has undergone a resurgence. It first appeared in Australia in 1994.48

PMMA was reportedly first synthesised in 1938,49 and it has been reported in some literature as being available since the 1970s.50 Compared to PMA, there are fewer studies available on the history of PMMA, and it is unclear when the drug emerged in Australia.

The trend of combining PMA with PMMA for sale as ‘ecstasy’ has been identified in Europe since the year 2000.51 It is unclear when PMA and PMMA began to be combined in Australia.

The United Nations Office on Drugs and Crime (UNODC) reported that PMMA had not been reported in ecstasy pills in Oceania in its 2013 World Drug Report.52 Despite this, the compound has been identified by the Crime and Corruption Commission (CCC) as being present in Queensland.53
Generally, there does not appear to be a specific market of people wanting to buy and consume PMA and PMMA specifically, although there is some evidence to suggest that there may be, or may have been, a PMA market in South Australia. It has been speculated that PMA and PMMA re-emerged on the illicit drug market in recent times because the precursors to make PMA and PMMA are easier to obtain than MDMA/‘ecstasy’ precursors.

PMA and PMMA are said to have less euphoric effects than MDMA/‘ecstasy’ and are slower to take effect. They affect people by making them alert and excited, heightening their senses and making them see colours and shapes. In addition to being sold under ecstasy-type brand names like ‘Mitsubishi’ and ‘E’, PMA and PMMA are also known as ‘Death’, ‘Dr Death’, ‘Red Mitsubishi’, ‘Pink Ecstasy’, ‘Killer’, ‘Chicken Powder’ and ‘Chicken Yellow’.

Another drug analogue detected in Queensland is Alpha-PVP, which has recently gained significant media attention in the United States as a drug known as ‘flakka’ or ‘gravel’. It is a stimulant that is also a member of the synthetic cathinone family. It is typically swallowed, but may be injected. The Australian Drug Foundation notes that there have been reports of use of Alpha-PVP in Australia, but its use does not appear to be widespread. Alpha-pyrrolidinovalerophenone (Alpha-PVP) is classified in the Drugs Misuse Regulation as a Schedule 2 dangerous drug.

There are many other drug analogue stimulants available in Queensland including:

- 3-trifluoromethylphenylpiperazine (TFMPP)
- Methiopropamine (MPA)
- 3,4-Dimethoxymethamphetamine (DMMA)

There are currently 47 synthetic stimulants listed in Schedule 2 of the Drugs Misuse Regulation.

**Hallucinogens**

Hallucinogenic drug analogues are drugs that produce a similar affect to psychedelic drugs like LSD. Drug compounds such as N-methoxybenzyl or ‘NBOMe’ have come to prominence in recent years in this drug class.


Some of the effects of NBOMe compounds on users include hallucinations, feeling happy and relaxed, heightened senses, increased sex drive and feelings of empathy. NBOMes typically come in the form of blotting paper, liquids, powders or pills, and they are taken by holding them under the tongue or in the cheek, or snorting.

Drugs from the 2C family are also popular in Queensland. These drugs include 2C-B (which has been marketed as a legal alternative to ecstasy since the 1980s), 2C-T-2 (which is also reportedly similar to MDMA/‘ecstasy’ but with greater hallucinogenic effects), 2C-I (which reportedly has stronger hallucinogenic effects than ecstasy and is quicker to take effect than other 2C drugs), and 2C-E (which reportedly enhances music and visuals for the user).

Other forms of hallucinogenic drug analogues in Queensland include:

- N,N-dimethyltryptamine (DMT)
- N,N-dialyl-5-methoxytryptamine (5-MeO-DALT)

There are currently 55 synthetic hallucinogens listed in Schedule 2 of the Drugs Misuse Regulation.

Although these are some of the commonly known drug analogues, new substances are constantly being developed and marketed.
The new definition of ‘dangerous drugs’ is intended to catch newly developed and marketed drug analogues; however, the majority of the drugs considered above are now specifically listed as either a Schedule 1 or a Schedule 2 ‘dangerous drug’ in their own right.

**Adverse effects on the user**

Many drug analogues have only been available on the global and Australian illicit drug market since the mid-2000s. As such, very little is known about the long-term health consequences of the use of these drugs. In addition, new substances are constantly being developed and marketed in an attempt to avoid drug regulations. These are quickly placed on the market with minimal or no testing on their suitability for use and consumption.

Although the long-term effects of drug analogues are largely unknown, there are a number of concerning adverse health effects associated with short-term use of the drugs.

Cannabimimetics are the most popular drug analogues in Queensland and Australia, and they have been associated with a number of negative symptoms including seizures, weight gain, respiratory problems, convulsion, fast or irregular heartbeat, paranoia, agitation, anxiety, psychosis, chest pain, vomiting, and kidney injury. Cannabimimetics have also been linked to cases of dependence. In some instances, the drugs have been associated with heart attacks, suicide, and stroke.

In Queensland, there have been a number of deaths linked to the use of cannabimimetics. In January 2015, two men died in Mackay shortly after using a cannabimimetic. The men died in separate incidents within days of each other, but it is believed that they used the same brand of drug. A Mackay woman was also placed in intensive care the following week after using the same cannabimimetic. However, the exact role played by the cannabimimetic in these incidents is unknown.

These deaths followed a number of warnings issued by the Mackay Hospital and Health Service regarding the effects of smoking cannabimimetics. In October 2014, the hospital issued a media release warning of the increase in people presenting with psychosis symptoms after smoking or ingesting such substances. A month later, the Mackay Hospital and Health Service warned it had treated seven people in less than a week for symptoms exhibited after using cannabimimetics. Two patients were admitted to the Intensive Care Unit. The patients exhibited nausea, vomiting, high blood pressure, irregular heartbeats and disturbed psychotic symptoms.

The Commission is aware that as early as June 2013, the then-State Coroner outlined concerns to Queensland’s Chief Health Officer regarding four deaths in the state thought to be linked to cannabimimetics. The negative effects of cannabimimetic use has led some researchers to conclude that the drugs are potentially more harmful than traditional cannabis. The severe negative effects that have on occasion arisen in regard to the use of cannabimimetics is of particular concern, given that use of the drug is most common in the 14-19 year age group.

Mephedrone has also been associated with a number of negative health effects. Some of these effects include anxiety, paranoia, restless sleep, jaw clenching, teeth grinding, light-headedness, dizziness, memory loss, nose bleeds, dilated pupils, blurred vision, dry mouth, sweating, reduced appetite, stomach pains, nausea, vomiting, skin rashes, fast heartbeat, high blood pressure, craving for more of the drug, chest pain, tremors and convulsions. Mephedrone has also been associated with dependence, and deaths linked to mephedrone have been reported in Sweden, the United Kingdom and Romania. However, the role that other substances and factors played in some of those deaths is unknown.

A number of negative health effects have also been associated with MDPV. The World Health Organisation has indicated that MDPV shows a high potential for abuse, with effects of the drug ranging from severe agitation, violent behaviour, a fast heart rate, sweating, psychosis, paranoia and anxiety.

MDPV has also been associated with a number of fatalities. In Queensland, MDPV is thought to have played a role in five deaths in the period between 2011 and 2014 in Mount Isa, with three of those deaths occurring between November 2013 and January 2014.
A 2014 report by the European Monitoring Centre for Drugs and Drug Addiction associated 108 deaths, reported to it by member states, with the presence of MDPV. They also noted that some studies have found a further 33 deaths linked with the drug in the United States, one death linked with MDPV in Japan, and a further 17 deaths associated with the drug in the European Union.

PMA and PMMA have been associated with the following adverse health effects: kidney failure, high body temperature, vomiting, convulsions, seizures and comas. Although often sold as MDMA, PMA and PMMA have a higher risk of acute affects and overdose than MDMA. By 2003, PMA had been associated with 40 reported deaths worldwide, either alone or in combination with other drugs. Between 1995 and 2003, ten deaths were associated with PMA in South Australia, Western Australia and Queensland.

In regard to PMMA, it was implicated in a death in Spain in 1993 in conjunction with other drugs that did not include PMA. Four of the 40 worldwide deaths associated with PMMA involved the presence of PMMA. In Israel, 24 deaths were also linked with this combination in 2007-2008. A recent Canadian study linked 27 deaths in Alberta and British Columbia between June 2011 and April 2012 to use of PMMA. In most instances in that study, PMA and other drugs were also present in the toxicology results to some degree. Other deaths have been associated with the drug in Germany and Taiwan. In 2012, three deaths in Queensland were reportedly associated with ‘ecstasy’ tablets containing PMMA.

Alpha-PVP has been associated with elevated body temperatures and heart rate, jaw clenching, vomiting and paranoia. In 2013, the New South Wales Coroner found that that a man died of cardiac arrest and fluid on the brain as a result of consuming Alpha-PVP in 2012, which he had purchased from an adult store.

---

**Case study**

**Person P**

This case resulted in a coronial inquest into the death of P, who died aged 44 at the Prince of Wales Hospital, Sydney, on 23 October 2012. He was a truck driver and was in a relationship with H. P and H were recreational users of drugs who heard about synthetic drugs being sold at a Nauti and Nice Store. These drugs were marketed by the store as ‘legal highs’. The Local Area Health District had declared these drugs were ‘legal but lethal’. When P and H approached the shop assistant about these, they were told that they were legal, but ‘with the sensation you get from an illegal drug’. They were advised to inject the drug which they subsequently did.

After the first use of the purchased drug, P’s behaviour became very strange and H disposed of the remainder of the drug. Regardless of this initial reaction, they both purchased and used the drug on several further occasions. H gave evidence at the inquest of the following side effects she suffered: feeling very hot, heart racing, feeling dehydrated. She also spoke of hallucinations such as seeing people in the house waving their hands at her, in the bath and under the beds. She said she suffered extreme fear and paranoia.

On the day of P’s death, he had purchased the drug, returned to the truck, and mixed it with water before injecting the drug into both himself and H. H fell out of the truck, as did P. By that stage, P had taken all his clothes off. They each ran down the highway in opposite directions. P was naked and H had her shirt off. They were yelling and stumbling across the road. H was cared for by motorists who stopped to assist. P ran towards a shipping yard, where he scaled an eight foot security fence covered in barbed wire. He was then seen to be running around manically before running into another building. The security guard witnessed him hitting a glass door with a ladder. A struggle ensued and although they were similar sizes, P showed extraordinary strength. After a further person came to the assistance of the security guard, they were ultimately able to restrain P. P continued to struggle and was displaying ‘super strength’, before
foaming at the mouth and then going limp. They then commenced CPR on him until the ambulance arrived. He never regained consciousness.

The evidence was that the cause of death was drug toxicity, and the drug found to be present in P’s system was Alpha PVP. The evidence from the stores selling the drug was that they were making up to $7,000 daily at the height of sales. A sales assistant gave evidence that she had witnessed the manic behaviour of those who had used the drug. On one occasion, a woman asked her if she could ‘eat her face’ before going outside to the road and eating from a dead animal.

At the time, Alpha PVP was not specifically prohibited under New South Wales’s drug laws. It has since been listed in the relevant legislation.

This case study provides a clear example of the alarming potential effects of this particular synthetic drug, and the dangers associated with drug analogues being sold and used in the community. It is difficult for legislatures to keep pace with the unrelenting and rapid emergence of drug analogues onto the market, and sometimes a new substance does not come to the attention of authorities until an event such as the above case occurs. Even though a new synthetic substance may be illegal under the extended definition of ‘dangerous drug’, if the substance is not specifically listed in the relevant legislation, it creates a potential for ambiguity for retailers and purchasers in knowing whether a substance is prohibited. It is vital that dangerous substances are identified and specifically included in legislation as quickly as possible.

NBOMe compounds have also been associated with negative health effects. These include confusion, difficulties communicating, nausea, exhaustion, restless sleep, agitation, aggression, eye spasms, paranoia, fear, panic, difficulty urinating, rapid heart rate, difficulty breathing, rapid breathing, hyperthermia, numbness, swelling, blue fingers and toes, and seizures.113

In March 2012, a number of university students in Queensland were hospitalised after using a product purchased as a ‘research chemical’. It was found to contain compounds from the NBOMe family.114 One of these students remained in a coma for three days.115 In 2014, a number of people were hospitalised in the Northern Territory after taking a ‘snapchat’ pill, which contained the compound 25I-NBOMe.116

In Australia and around the world, the NBOMe family has been associated with a number of deaths. NBOMes were reported to be responsible for four deaths between March 2012 and January 2014 in Australia.117 Three of these deaths were teenage school students.118

Case study

Person K119

K was a 17-year-old boy in Grade 12 in New South Wales. K was a hard-working and high-achieving student, who was likely to be dux of his school. He had been ill recently and felt he needed to spend more time catching up on his studies prior to his exams. It appears that K purchased a tablet from a school friend, who had received the drug from a person who had purchased it off the Internet. There was some talk around school that it would help with studies.

On the day of K’s death, his mother picked him and his sister up from school. K was dropped home while his mother and sister went shopping. At that point, K was acting normally. When his mother and sister arrived home an hour later, K was extremely agitated and talking a great deal at an extremely high speed. He then went into his room and started throwing bottles onto the floor. His mother was distressed by this behaviour and ordered him to stop. K walked outside the room and vomited on the ground. His mother then put him in the shower, and at that point he apologised to his mother, telling her he had taken something. He asked her to please call his father and apologise for him. Though he was in a psychotic
state, he was still clearly ashamed of his actions. She did not understand what he was talking about. After having a shower, he then got dressed before again undressing and curling into a foetal position on the floor, rocking back and forth. He then exclaimed that he wanted to fly. He ran out onto their third floor balcony and attempted to jump off. His mother and sister attempted to restrain him, causing him to bite his sister, seemingly not knowing who she was or what she was doing. He then fell to his death.

Following his death, it was revealed he had taken 251-NBOMe, a hallucinogen estimated to be 25 times more potent than LSD. That drug was not illegal at the time; however, it has now been included as a dangerous drug in the New South Wales’s drug legislation.

In a number of 2014 reports, the World Health Organisation attributed NBOMes to ‘a number’ of deaths in Australia, in addition to deaths in Belgium, Poland, Switzerland, the United Kingdom and the United States.120 The United States reported 14 deaths—some of which were due to acute toxicity, while others were due to unpredictable, violent behaviour after taking the drug.121

There is limited information available on the effects of drugs from the 2C family. Some adverse consequences of 2C drug use have been reported as vomiting, agitation, rapid heart rate, high blood pressure, hyperventilation and seizures.122 A 2013 study of the drugs found that at least five deaths had been attributed to the 2C family, but did not further elaborate on the circumstances of these deaths.123

Some of the severe effects of drug analogues have been put down to the fact that the active ingredients in these products are often unknown and untested—or poorly tested—on humans.124 Another explanation for their severe negative effects are that the ingredients listed on the product are not often a true reflection of the actual contents of the package.125 In some instances, none of the listed ingredients have been found to be present in the packaged substance.126 This means that those taking the drugs may be misled by the contents or are simply unaware of what they are consuming and the danger or toxicity of those substances.

Drug analogues can often be inconsistent across batches.127 A person who has previously used a brand of drug may incorrectly rely on having a similar response, tolerance, effect or required dosage when a different batch of the same brand may in fact have a higher potency.

Another factor that may contribute to the fatalities and hospital admissions associated with drug analogues is that they are often more potent than the drug they are intended to mimic,128 with required dosages varying considerably. This leads to a greater risk of overdose. For example, NBOMe, which has been compared to LSD and ‘ecstasy’, has been reported as being active at 0.05 mg; this compares to a ‘dose’ of ‘ecstasy’ which is around 125 mg.129 Similarly, cannabimimetics have often been reported as being more potent than traditional cannabis.130 Professor Iain McGregor, Professor of Psychopharmacology at the University of Sydney recently stated, ‘Natural cannabis tends to tickle the receptors whereas the synthetic cannabinoids tend to bash them’. The analogy of drinking a schooner of beer as opposed to a schooner of straight vodka has also been made.131 The dosage for MDPV is about 100 times smaller than it is for mephedrone.132 This is dangerous, as both drugs are commonly sold as ‘bath salts’. A further risk of MDPV is that its dosage is measured in milligrams, which means there is a small margin between a ‘safe’ dose and a lethal dose.133

In addition to being more potent, some drug analogues may be slower to take effect. This means that some users may re-dose to achieve an immediate effect, which may ultimately lead to an overdose.134 This risk is higher when a drug analogue has been sold as another illicit drug. For example, PMA or PMMA are sometimes sold as MDMA or ‘ecstasy’. However, PMA and PMMA are more toxic than MDMA and are slower to take effect.135 This may lead to people to mistakenly thinking that the ‘ecstasy’ is weak when they do not feel the effects as they normally would, and they may unwittingly overdose by taking further amounts of the drug without realising they are not using MDMA.136

Users of drug analogues are risking exposure to a number of negative side effects, serious illness and potentially death. The lack of information on the long-term effects of the use of these drugs is of great concern, particularly where products such as cannabimimetics are being used by teenagers who may be...
The illicit drug market

Queensland Organised Crime Commission of Inquiry

vulnerable on account of their inexperience, and also because their brain is still in a stage of development. A New South Wales Emergency Department doctor has been quoted as saying 'Oh, for the good old days of heroin and cocaine... At least then we knew what we were dealing with and how to treat it.'

The prevalence of synthetic drugs within the community

The prevalence of synthetic drugs globally

Globally, drug analogues have been detected in every region of the world. In 2014, there were 450 different drug analogues known to be available globally. This was more than double the 216 drug analogues that had been identified in 2012, although some of the increase is due to an expansion in the data sources.

In the first half of 2012, 44 drug analogues were detected in the Oceania region, which was equivalent to more than a quarter of all drug analogues identified worldwide in this period.

Cannabinimetics appear to be developing the most rapidly. In mid-2012, there were 60 identified synthetic cannabinoids world-wide. By 2013 this had increased to 110, and in 2014 there were 177 different synthetic cannabinoids reported to the UNODC.

A survey of youth in the European Union found that in 2011, 3.6 per cent of people aged 15–18 years had tried drug analogues, with 5.6 per cent in the 19–21 year and 22–24 year age groups having tried them. Drug analogues are particularly popular in Ireland, where 16.3 per cent of those aged 15–24 years had tried them in 2011. Use of traditional illicit drugs in Europe, aside from cannabis, appears to have remained stable between 2003 and 2011, but use of drug analogues has increased.

Despite the popularity of the drugs between 2011 and 2013, there have been some recent indications of a decline in the popularity of drug analogues in some regions. For example, in the United States, use of cannabinimetics among twelfth-grade students halved between 2012 and 2014, and use of mephedrone in the United Kingdom among those aged between 16 and 24 years fell by almost two thirds from 4.4 per cent in 2010–2011 to 1.6 per cent in 2012–2013. It is unclear at this stage whether this indicates a general downward trend for use of drug analogues globally.

In a 2012 survey conducted by UNODC, Asia was nominated by regions seizing drug analogues as the primary source of the drugs, with East and South-East Asia appearing to dominate the industry. Drug analogues in Asian markets also appear to originate domestically. Europe was nominated as the second-most dominant source of the drugs. Few countries reported domestic production of the drugs, meaning that the drug analogue market generally relies on overseas imports.

The prevalence of synthetic drugs in Australia

Despite the rapid expansion of drugs available on the drug analogue market, their use throughout Australia remains relatively low. According to the National Drug Strategy Household Survey, in 2013, 1.2 per cent of the population had used a cannabinimetic in the past 12 months, with 0.4 per cent using other synthetic drugs in that period. This is lower than the use of other drugs such as cannabis, ‘ecstasy’, amphetamines and cocaine, but higher than some other traditional illicit drugs such as heroin and GHB.

Use of cannabinimetics is most popular in the 14–19 year age group, followed by 20–29 year-olds. This shows a younger pattern of use than most other illicit drugs, which are used more commonly by the 20–29 year age group. Use of other drug analogues was consistent with illicit drug use generally, predominately by those in the 20–29 year age group.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Per cent of population using cannabimimetics and other new psychoactive substances in their lifetime and in the past 12 months (2013)

![Bar chart showing per cent of population using cannabimimetics and other new psychoactive substances in their lifetime and in the past 12 months (2013).]


Although the National Drug Strategy Household Survey provides useful information on drug use in the community, it is unable to shed any light on drug analogue trends, since drug analogues were included in that survey for the first time in 2013.

Studies conducted on drug analogue use by illicit drug users can shed some light on drug analogue trends in recent years. A 2014 study indicated that drug analogues are particularly popular among ‘ecstasy’ and other psychostimulant users. The study showed that 40 per cent of regular ‘ecstasy’ users in Australia had used a drug analogue in the six months prior to their interview.158

Although not representative of the general community, these studies shed some light on the popularity of the drugs among those engaged with the illicit drug market.

The popularity of drug analogues is also reflected in the national drug seizures. Seizures of drug analogues by the Australian Federal Police recently increased, with 56 seizures totalling a weight of 146 kilograms made in 2012–2013, increasing to 96 seizures weighing a total of 543 kilograms in 2013–2014.159 Despite cannabimimetics being the most commonly used drug analogues in the country, seizures were mainly of stimulant drug analogues.160 In 2014, there was a decline in seizures of cannabimimetics in Queensland.161

Prevalence within Queensland

The Crime and Corruption Commission (CCC) has noted that:

[the synthetic drug market is] one of the most rapidly evolving illicit drug markets... More new substances have been identified in the past five years than in the last fifty years combined, with an average of one new substance detected every week.162

The CCC has rated the risk assessment of this market to the Queensland community. This market was first rated in 2009 with a low level of risk, and in 2013 this level was adjusted to medium with an increasing trend.163
In Queensland, 55 new substances were detected by the CCC between mid-2011 and May 2012. In a 2014 report, UNODC was aware of 450 different drug analogues being sold globally, with 97 of these drugs coming to their attention in the period between July 2012 and December 2013.

Drug analogues, with some exceptions, first emerged on the Queensland market in 2007 and were identified by the CCC as a threat in 2009. Since 2009, the CCC has seen an ‘explosion’ in the number and variety of synthetic drugs available in Queensland. The CCC reports that drug analogues are imported into some parts of Queensland on a weekly basis.

Although drug analogues are available to consumers all through Queensland, the CCC has found that they are most prominent in northern and central Queensland. In particular, synthetic drugs have been detected in high rates in the Mount Isa region.

Some of the popularity of drug analogues in northern and central Queensland has been attributed to the localisation of mine employees in those areas. There are a number of reasons for the popularity of these drugs in the mining regions. For one thing, the nature of synthetic drugs is rapidly changing. Additionally, difficulties in effectively testing employees for drugs makes it challenging for employers to detect such rapidly changing drugs. Further, those residing and working in mining communities generally have a higher income and thus a greater capacity to pay for these new drugs.

Cannabimimetics are the most popular of the drug analogues in Queensland. Between October 2013 and March 2014, the majority of synthetic cannabis-related arrests occurred in the Northern region and the South Eastern regions of Queensland.

MDPV has increased in availability in Queensland recently, with the drug particularly popular in the Mount Isa region. A number of deaths in Mount Isa have been attributed to the drug. Alpha-PVP has also been detected in Mount Isa since 2012.

Drugs from the NBOMe group have also increased in use and availability in Queensland recently, having first been reported in the state in 2012. Drugs from the 2C hallucinogen family have been available as early as the 1980s, with others such as 2C-T-2 only appearing in Queensland in 2013. The 2C-B and NBOMe drugs have been found to be reasonably popular with regular ‘ecstasy’ and psychostimulant users in Queensland.

Although PMA has been available in Queensland for some time, it is unclear how long PMMA or the combination of PMA and PMMA have been on the market. However, as far back as 2012, three deaths were linked to the use of PMMA in Queensland. Recently the QPS issued a statement warning the public about the dangers of a ‘Superman’ tablet thought to contain ‘deadly amounts of PMMA’ which may have become available in Australia.
Studies conducted on drug analogue use by illicit drug users can shed some light on drug analogue trends in recent years in Queensland. A 2014 study indicated that drug analogues are particularly popular among ‘ecstasy’ and other psychostimulant users. In Queensland, 57 per cent used a drug analogue in the six months prior to their participation in the study. Drug analogues were more likely to have been used recently by regular ‘ecstasy’ users than were methylamphetamine powder (speed) and methylamphetamine crystal (ice). This was an increase from 2013, where 49 per cent reported use of a drug analogue in the six months prior to their interview in Queensland.

This shows that among MDMA/‘ecstasy’ users who already have a propensity to use synthetic drugs, drug analogues are growing in popularity, and their use is surpassing the use of other illicit drugs among this group in Queensland.

A study on injecting drug users also found higher rates of drug analogue use than among the general population. In Queensland, 21 per cent of injecting drugs users had tried cannabimimetics, with three per cent using cannabimimetics in the six months prior to the 2014 study. In 2013, although lifetime use of a cannabimimetic was lower at 16 per cent, seven per cent had used the drug recently, which is a higher percentage of recent use than in 2014. In the same study, sixteen per cent of Queensland respondents reported using a non-cannabimimetic drug analogue in their lifetime, with four per cent using recently in 2014. This was an increase from six per cent of injecting drug users reporting having tried drug analogues in 2013. The amount of injecting drug users recently using a non-cannabimimetic drug analogue was four per cent, with that figure remaining stable.

Although lifetime use among injecting drug users of drug analogues increased in Queensland, the recent use of drug analogues remained relatively stable and, in the case of cannabimimetics, decreased—indicating that drug analogues were not as popular among this group. It may also indicate that users are turning away from cannabimimetics, as regular use decreased between 2013 and 2014.
The illicit drug market

The emergence of this market and the appeal of drug analogues to young people has been attributed to a number of factors including:

- The marketing of drug analogues as ‘legal’, despite being illegal in many locations around Australia and the world.\(^{192}\)
- The marketing of drug analogues as ‘safe’, or the implication that they are safe as evidenced by their apparent legal status.\(^{193}\)
- The easy availability of drug analogues over the Internet, and the use of aggressive marketing tactics by sellers, such as discounts for buying in bulk and reward point systems.\(^{194}\)
- The fact that drug analogues are accessible—or have been accessible until recent times—at retail outlets such as drug paraphernalia stores, tobacco shops and adult stores.\(^{195}\)
- The free availability of information about new drugs, new brands and the effects of drug analogues on the Internet, including in user discussion forums.\(^{196}\)
- The marketing of drug analogues using brand names, sophisticated packaging and references to popular culture.\(^{197}\) (For example, drugs recently seized in the Northern Territory containing an NBOMe compound were stamped with the logo for the popular social-media platform ‘Snapchat’).\(^{198}\), which may make them attractive to young people and give them a sense of legitimacy.
- The low risk of detection in routine drug tests.\(^{199}\)
- The lack of availability of traditional drugs in regional areas.\(^{200}\)
- The decrease in availability of MDMA/‘ecstasy’ since 2008 and the need to find substitute substances (It should be noted that in recent times the MDMA/‘ecstasy’ market has undergone a resurgence).\(^{201}\)
- The lower risk of law enforcement detection\(^{202}\) because of the sheer number of packages sent by international mail entering the country.\(^{203}\)
Part of the popularity of drug analogues has also been attributed to their affordability. Drug analogues in Queensland are either priced at a similar cost to the drugs they mimic, or are slightly cheaper. For example, participants in the Ecstasy and Related Drug Reporting System in 2014 indicated paying between $1 and $50 for a tab of LSD, and between $0 and $25 for a pill of NBOMe. There have been some reports of drugs mimicking LSD that are available online for as little as $2 a tab when bought in bulk.

There are indicators in Queensland—and around the world—that there has been a recent decline in the use of drug analogues. The CCC has recently noted a decrease in the Queensland drug analogue market, following a resurgence of the availability of MDMA/‘ecstasy’. It is unclear at this stage if this decline will be a continuing trend, or whether the decline is linked to increasing regulation of the drug analogue market.

The CCC is of the view that the drug analogue market is beginning to replicate the traditional illicit drug market, following the introduction of amendments to the Drugs Misuse Act.

Detective Inspector Slater of the QPS Drug Squad, in an interview with this Commission, confirmed that the police continue to see the existence of these type of drugs in adult and tobacconist shops within Queensland. The QPS earlier this year executed warrants across Queensland, resulting in charges being laid against a number of the proprietors of these stores for selling synthetic drugs.

**Recommendation**

3.3 The Commission recommends that the Queensland Police Service consider increasing the number of operations targeting drug analogues in mining regions in Queensland, given the prevalence of drug analogues in these regions and the apparent inability of mining companies to test for such ever-evolving drugs.

What role does organised crime play in the new synthetic drug market within Queensland?

The drug analogue market is not dominated by organised crime groups. However, according to the CCC, this market is increasingly mirroring the traditional illicit drug market in Queensland, and organised crime groups are becoming more involved in the importation and distribution of these drugs.

The Internet is one of the main sources of supply for drug analogues to users in Australia. Customs seizures indicate that most seizures of synthetic drugs are either in small ‘personal use’ quantities or in larger shipments that reflect an intention for on-selling. The evidence and information available would suggest that those who buy in bulk and distribute the substances are not typical players in the illicit drug scene, and do not usually have experience in the illicit market. They are more commonly young people of an entrepreneurial nature.

In Queensland, there are increasing networks of persons buying synthetic drugs in bulk online for on-sale, either directly to users or to street dealers. There is information that, where groups are aware that law enforcement authorities are targeting a particular area (for example, targeting MDPV in Mount Isa), they have arranged for the product to be sent to an alternative area that is not being targeted. Arrangements are then made to transport the product from that place to its ultimate destination, in an attempt to avoid detection by authorities.

There is also evidence that drug analogues are being commercially produced in Queensland. Charges have been laid against individuals for producing drug analogues; however, given that those matters are subject to current judicial proceedings, this Commission—in accordance with its Terms of Reference—is prohibited from further examining the behaviour of these individuals.

Chemical synthesis of the drugs themselves is rare in Queensland, and the CCC predicts that this will continue to be the case while drug analogues can be purchased easily online from overseas producers.
Although there is a pattern of new, entrepreneurial individuals and networks in the drug analogue market, there have been some reports of traditional organised crime groups—such as outlaw motorcycle gangs—being involved in the distribution of drug analogues in Queensland.221

Recently, there has also been an increase in the level of sophistication in concealing the importation of drug analogues. The Commission is aware that there have been practices being developed by people in an attempt to avoid detection by the authorities. Some of these include limiting imports to a certain monetary value to avoid reporting requirements, sending parcels to false addresses, using prepaid credit cards which, therefore, avoid the necessity of providing identification over the Internet, and communicating through chat rooms, Skype, gaming consoles, blackberry and various social media platforms which makes it very difficult for the authorities to trace.222 The drugs are also being concealed in other goods such as tea, power regulators and liquid solutions.223

The Australian Crime Commission considers that there is currently a low level of involvement of organised crime groups in importing and supplying drug analogues to consumers in Australia.224 It is noted, however, that as the market expands, the potential for organised crime to become heavily involved in this market is of concern.

Although this market is not currently a stronghold for traditional organised crime groups, it is believed that if the market remains profitable—and the demand for these drugs increases—then organised crime groups, entrepreneurial individuals and networks will continue to be involved in (and will increase their involvement with) the supply of drug analogues.

Conclusion
The emergence of drug analogues into the Queensland market is of great community concern, given the potential for significant ramifications from their use. While the use of drug analogues across Queensland is not currently as widespread as the use of other illegal drugs, law enforcement is concerned that drug analogues will increase in popularity as they become more well-known and widely available. For government and law enforcement, drug analogues are insidious; as one is identified and placed onto the schedule in the Drugs Misuse Regulation, a slightly modified substance becomes available.

While successive Queensland Governments have been alert to the issue and have attempted to address the problem by extending the definition of ‘dangerous drug’ in the Drugs Misuse Act to apply to analogues of scheduled substances, such prosecutions can be difficult.

Most drug analogues recognised in Queensland have been listed as Schedule 2 dangerous drugs in the Drugs Misuse Regulation—with the exception of PMA and PMMA, which are included in Schedule 1 (and hence subject to greater maximum penalties). Given the serious consequences—including death—that can flow from the use of drug analogues, the schedule classification of drug analogues is an issue that warrants further examination. The issue is further examined in the following section, entitled 'Legislation'.

(Endnotes)


The illicit drug market


7 Explanatory Notes to the Criminal Law (Child Exploitation and Dangerous Drugs) Amendment Act 2013. p. 3.

8 Sections 40(2) & (3) Criminal Law (Child Exploitation and Dangerous Drugs) Amendment Act 2013 (Qld).

9 Section 4 Drugs Misuse Act 1986 (Qld).

10 Statutory Declaration of Michael Walsh, 28 August 2015, para 15.

11 Statutory Declaration of Ross Barnett, 27 August 2015.

12 Transcript of Interview, Mark Slater, 1 July 2015, p. 13. [In - Confidence].


25 Statutory declaration of Michael Walsh, 28 August 2015, para 22.


assessments of PMMA in the framework of the joint action on new synthetic drugs. Lisbon: European Union, p. 75.


3 The illicit drug market

Queensland Government, pp. 24, 25 [In-Confidence].

66 Statutory declaration of Michael Walsh, 28 August 2015, para 22.


74 Statutory declaration of Michael Walsh, 28 August 2015, para 22.


The illicit drug market

Queensland Organised Crime Commission of Inquiry


Mackay Hospital and Health Service. (2014, October 30). Mackay medical specialists warn against synthetic drugs. Media Release.

Mackay Hospital and Health Service (2014, November 21). Doctors renew warning against smoking synthetic cannabis. Media Release.

87 Letter of Crown Law for Queensland Health, 28 July 2015, attaching copy of letter of Mr Michael Barnes (then State Coroner) to the Chief Health Officer, Dr Jeannette Young, dated 12 June 2013.


outbreak in Israel. Clinical Toxicology, 50, 39–43.


3 The illicit drug market


The illicit drug market

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>
The illicit drug market

Queensland Organised Crime Commission of Inquiry


210 Transcript of Interview with OCCOI, Detective Inspector Mark Slater, 1 July 2015, p. 13. [In-Confidence].


3.3 The effect of illicit drug use on society

Illicit drug use not only affects the drug user but also the wider community in a number of different ways. The community may feel the effects of illicit drug use through government expenditure on drug-related services and resources as victims of drug-related crime, or through risks to their safety presented by people under the influence of drugs or who are producing drugs.

In addition to affecting the broader community, those close to illicit drug users are particularly at risk of exposure to negative experiences due to their relationship and association with the drug user. Those closest to illicit drug users—such as the users’ children, parents, siblings and extended family—are often more adversely affected by illicit drug use than are other members of the community. How they are affected by this drug use may depend on the frequency and extent of the drug use, the type of drug used, and the closeness of the relationship that the person has with the drug user.

Children in the care of a regular illicit drug user may suffer particular disadvantage as a result of parental drug use or dependency. These disadvantages may start from conception, in instances where a mother uses drugs during her pregnancy, and continue into their adult life. Children of drug users may suffer from adverse health consequences, neglect or abuse, or poor educational outcomes, or they themselves may be susceptible to drug use in adolescence or adult life.
Family members may also feel abandonment, anxiety, fear, anger, concern, embarrassment or guilt as a result of a family member using drugs. Siblings may also feel overlooked by parents who are preoccupied with a drug-abusing sibling.

Family, friends and co-workers may be affected because the user may be unreliable. Friends may be asked to help the user financially, and co-workers may have to compensate for decreased productivity or they may have to carry a higher workload.

### 3.3.1 What effect does illicit drug use have on the community?

#### Health care

More broadly, illicit drug use touches on every member of the community through the allocation of funds and resources. One of the main areas of funding is health care. Illicit drug use increases the burden on public and private health care providers, diverts resources away from other medical conditions, and comes at a significant financial cost to the public.

Illicit drug use accounts for an increasing proportion of the global burden of disease. It is estimated that some 4.5 million people worldwide receive treatment for illicit drug use, at a global cost of about $35 billion annually.

In relation to illicit drug treatment in Australia, using data from the 2010–2011 financial year, Smith et al. determined that:

- 13,849 public hospital admissions had a principal diagnosis related to illicit drugs
- 6,928 private hospital admissions had a principal diagnosis related to illicit drugs
- 65,376 closed episodes occurred for alcohol and other drug treatment services
- 10,801 finalised residential episodes occurred for treatment of illicit drug use
- 46,446 people were in receipt of pharmacotherapeutic treatment.

Smith et al. also attempted to estimate a cost to the Australian society for illicit-drug-related health care. The total costs of illicit drug use treatment were estimated to be $605 million for the year 2011, excluding loss of productivity costs.

The total estimated illicit-drug-related hospital costs for public hospital stays and presentations at emergency departments for that year were estimated at $112 million.

There were also 6,928 private hospital admissions related to illicit drug use in the 2010–2011 financial year and emergency department presentations at private hospitals. Approximately 55 per cent of private costs were funded from governments and individuals. As such, this ratio was used to estimate a cost to society for these private hospital attendances of $20 million for illicit drug use.

The cost of residential drug treatment for amphetamines, cannabis, cocaine, MDMA/‘ecstasy’ and opioids was estimated to amount to $174 million. The costs of community-based treatment related to illicit drug use, based on figures for treating community-based mental health patients, were estimated to be $114 million.

In addition, there were also illicit drug users in receipt of pharmacotherapeutic treatment such as methadone for opiate abuse. Smith et al. estimated the costs of this treatment to be approximately $185 million.

The total costs of these treatments are approximately $605 million.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Australia estimated costs of drug related healthcare 2011 - excluding loss of life and productivity costs


The $605 million attributable to illicit drug use does not include the costs of those injured by someone who is dependent on drugs, the costs of social welfare payments to those dependent on drugs, the intangible costs of drug use, and the resources that are put into raising community awareness regarding illicit drug use.14

The Commission considered in detail the Alcohol and Drug Treatment Services in Queensland Final report April 2015.15 While highly informative, the report was limited in its application to this Inquiry, given that most of the statistics relate not only to illicit drug-related problems, but also to problems associated with alcohol and nicotine use.

It has been estimated that between 39,380 and 46,987 individual clients seek treatment for an alcohol or drug-related problem in Queensland per year, based on 2012–2013 figures.16

The types of services that these figures are based on include: specialised alcohol and drug treatment services, opiate pharmacotherapy, inpatient treatment, consultation liaison services, emergency department presentations, and treatment within community mental health services.

In 2012–2013, there were an estimated 29,385 episodes of care in specialised alcohol and drug treatment services in Queensland.17

Of the 29,385 episodes, cannabis was the principal drug of concern in an estimated 10,050 episodes, amphetamines in 3,215 episodes, heroin in 1,102 episodes, ‘ecstasy’ in 331 episodes, cocaine in 65 episodes, and other stimulants and hallucinogens in 136 episodes.18
A breakdown of episodes by principal drug of concern is contained in the table below.

**Number of estimated closed treatment episodes - Queensland 2012-13**

<table>
<thead>
<tr>
<th>Codeine</th>
<th>Other sedatives and hypnotics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morphine</td>
<td>Amphetamines</td>
</tr>
<tr>
<td>Buprenorphine</td>
<td>Ecstasy (MDMA)</td>
</tr>
<tr>
<td>Heroin</td>
<td>Cocaine</td>
</tr>
<tr>
<td>Methadone</td>
<td>Nicotine</td>
</tr>
<tr>
<td>Oxycodone</td>
<td>Other stimulants and hallucinogens</td>
</tr>
<tr>
<td>Other opioids</td>
<td>Volatile solvents</td>
</tr>
<tr>
<td>Other analgesics</td>
<td>Cannabis</td>
</tr>
<tr>
<td>Alcohol</td>
<td>Other</td>
</tr>
<tr>
<td>Benzodiazepines</td>
<td>Not stated</td>
</tr>
</tbody>
</table>


Although data was not available for 2012–2013, as at 28 November 2014 there were 7,730 clients in Queensland receiving opioid pharmacotherapy treatment services. The majority of these clients were from private prescribers. Due to the date, caution should be exercised when considering this figure, although it does give a general indication of the number of people accessing pharmacotherapy at any one time.

In Queensland in 2013–2014, cannabis was the principal illicit drug for which treatment related to drug use was sought. It was the principal drug of concern in 34 per cent of drug- and alcohol-related closed treatment episodes (where treatment has ceased for at least three months). This is second only to alcohol, which was the principal drug of concern in 37 per cent of closed episodes. In 2010–2011, Queensland drug and alcohol information services also reported that the majority of inquiries they received were about cannabis.

In 2012–2013, amphetamines (not including ‘ecstasy’) were the principal drug of concern in 3,215 closed treatment episodes for drug use in Queensland. Behind cannabis, amphetamines accounted for the second-most closed treatment episodes out of the illicit drugs. Amphetamines accounted for 10.9 per cent of alcohol and drug treatment episodes, with treatment for alcohol and cannabis being the only other substances accounting for a greater per cent of treatment episodes.

Nationally, there were 22,265 closed treatment episodes for drug use where amphetamines were the principal drug of concern, with cannabis being the only other illicit drug accounting for more treatment episodes.

In Queensland, the estimated spending for 2012–2013 on alcohol and other drug services was $226,977,266, which is approximately 19.2 per cent of the national expenditure on alcohol and other drug treatment. Having regard to the proportion of treatment episodes where amphetamines are the principal drug of concern in Queensland, this treatment cost approximately $24,833,491. This figure is a general estimate and should be treated with caution, as the costs allocated to specific types of treatments sought by amphetamine users have not been considered.
These do not include figures for treatment of illnesses such as heart or kidney disease or hepatitis that may be related to a person’s use of methamphetamine, and only give a small indication of the costs to the health care system caused by amphetamine-type stimulants.

It should be noted that treatment figures and cost estimates for Queensland and Australia should only be used to gain a general indication of the extent of resources dedicated to drug and alcohol treatment. Comparisons between the Queensland estimates for 2012–2013, the national estimates for 2011–2012 and 2004–2005 should not be considered in comparison, as differing methodologies, available data, the inclusion of different substances and drug use patterns between the years and different states may impact the data.

Many of these studies do not include, or do not specifically refer to including, broader costs of drug use and dependency, such as the costs for treating drug-related diseases, or victims of drug-related violent crime. It is, therefore, likely that the true costs of illicit drug-related health expenses are far greater than the provided estimates.

Whichever estimate is used or preferred, it is clear that the economic costs of health care related to illicit drug use are a significant cost to the community.

**Criminal justice**

Another primary area of expenditure in relation to drugs is in the criminal justice system. In addition to expenditure on criminal justice, members of the community may also suffer as the victims of drug-related crime.

In 2014, the Queensland Police Service (QPS) recorded 32,035 drug possession charges, 466 drug trafficking charges, 2,076 drug production charges, 3,714 supply of drugs charges and 34,363 ‘other’ drug charges. This totalled approximately 72,654 charges directly related to drug offences in Queensland. To put this in context, in the same period in New South Wales, 51,508 drug offence ‘incidents’ were recorded.

Illicit drug users are often participants in broader offending behaviour than just the possession and supply of drugs. The 2013 National Drugs Strategy Household Survey reported that 1.6 per cent of people who had used illicit drugs in the 12 months prior to the survey had physically abused someone while under the influence of drugs. In addition, 3.8 per cent of recent drug users admitted to creating a disturbance, damaging goods or stealing goods while under the influence of drugs.

The Drug Use Monitoring in Australia program is a study that collects information on drug use and criminal behaviour from detainees (alleged offenders) in watch-houses across Australia. In 2009–2010, the program found that of 1,317 police detainees in Brisbane providing urine samples for drug testing, 65 per cent tested positive for at least one drug type. Cannabis was the most commonly detected drug, followed by benzodiazepines, opiates and amphetamines. Benzodiazepines are tranquillisers such as Xanax® and Valium® that are commonly prescribed by doctors to relieve stress and anxiety; however, these drugs are also used by some to become intoxicated or to help with the ‘come down’ effects of other illicit drugs. Only six detainees tested positive for cocaine.

Thirty-two per cent of Brisbane detainees providing a sample tested positive for more than one type of drug. Twenty-six per cent of Brisbane detainees providing a sample attributed their offending to drugs. Most commonly they attributed property and drug offences to use of drugs, followed by breach offences and then violent offences.
The illicit drug market

In addition to admissions of drug use by detainees, urinalysis on those offenders found drugs in the system of 75 per cent of alleged breach offenders, 67 per cent of alleged property offenders, 67 per cent of alleged drug offenders, 58 per cent of alleged drink driving offenders, 65 per cent of alleged disorder offenders and 54 per cent of alleged violent offenders.

The Drug Use Monitoring in Australia program also found that across Australia in 2009–2010, 66 per cent of the 5,714 detainees providing a urine sample tested positive to at least one drug. Cannabis was the most commonly detected drug with 46 per cent of detainees that provided a sample testing positive, followed by benzodiazepines in 23 per cent, opiates in 22 per cent, amphetamines (including methylamphetamine) in 16 per cent and heroin in 13 per cent of detainees.

Twenty per cent of detainees across Australia attributed their offending to drug use, which is slightly lower than the Brisbane attribution rate. Detainees most commonly attributed drug offences to their drug use, followed by property offences, breach offences, and violent offences.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Other offences
Breach offences
Disorder offences
Drug offences
Traffic offences
Variety offences
Violent offences

Table 7 – effect on society – criminal justice
Attribution of offending to drugs by detainees 2009-10 - National


For each category of offence, cannabis was the most commonly detected drug. However, opiate and benzodiazepine users were highly represented among alleged property offenders. Interestingly, although amphetamines (including methylamphetamines) are commonly associated with violence, amphetamines were the fourth-most commonly detected drug in violent offenders, being detected in 13 per cent of violent offenders behind cannabis (45 per cent), benzodiazepines (20 per cent) and opiates (14 per cent). It is noted by the Commission, however, that this data relates to offending behaviour and arrests that occurred in 2009–2010, when the current ice epidemic had not become as prevalent as it currently is.

Table 8 – effects on society – criminal justice
Detainee test results for drugs by alleged offence 2009-10 - National

Data from 2012 indicated that nationally, 32 per cent of offenders charged with a property offence tested positive to methamphetamine, and 21 per cent tested positive to methamphetamine for an offence of violence. In the 2012 data, positive tests for methamphetamine for offences of violence overtook the prevalence of benzodiazepines in violent offenders, which was detected in 17 per cent of detainees charged with a violent offence.

In a report on the costs of illicit drugs in 2003, Collins, Lapsley, & Marks attributed nearly a quarter of violent crime attracting a jail sentence to illicit drugs alone, or to illicit drugs used in combination with alcohol.

Other indicators of drug use and criminal behaviour include a study of ‘ecstasy’ and psychostimulant users in Australia in 2014. That study found that 14 per cent of respondents reported that they had committed a property crime in the month preceding their participation in the project. Twenty-three per cent of those having recently committed property crime did so once a week, eight per cent committed property crime more than once per week but less than daily, and three per cent committed property crime on a daily basis. Three per cent of respondents to the study had reported committing fraud in the month preceding the interview, and four per cent had reported committing a violent crime in the past month. For Queensland, three per cent of ‘ecstasy’ and psychostimulant users had committed property crime in the month before the interview, four per cent had committed a violent crime in the previous month, and three per cent had committed fraud in the previous month.

Similarly, a study of injecting drug users in Australia in 2014 found that 18 per cent of injecting drug users had committed property crimes in the month preceding their project interview, with four per cent committing fraud in the month before interview and five per cent committing a violent crime. In Queensland, 20 per cent of injecting drug users reported being involved in property crime in the past month, with six per cent reporting involvement in fraud and four per cent reporting involvement in a violent crime. These rates are generally higher than for ‘ecstasy’ and psychostimulant users.

In both studies, there was also significant involvement with users in drug-dealing offences committed in the month before interview.

These studies, although not establishing a causal link between drug use and crime, show that there is a clear representation of drug users among those committing crimes.

There are limited figures regarding exactly how much illicit drug use costs the Australian and Queensland society through the criminal justice system.

Collins and Lapsley estimated that for 2004–2005, the tangible costs of illicit drug-related crime were estimated to be approximately $3.84 billion. This figure was derived by considering the costs of policing, criminal courts, the costs of prisons, the foregone productivity costs to society by placing people in prison, the cost of property theft and damage, the administration of insurance and the costs of violence.

A 2011 examination of the criminal costs for cannabis offences to the New South Wales justice system similarly considered costs such as policing, courts, administering penalties, costs to the director of public prosecutions and costs to legal aid. In that report, costs related to cannabis enforcement alone were valued at approximately $49 million.

These figures should be treated with some caution as they are both dated, and each study had a number of unknowns. However, they demonstrate the broad range of economic costs incurred by the criminal justice system.

In addition to the economic costs of drug use, there are also physical, economic and emotional costs that may be suffered by victims of drug-related crime, particularly as a result of property theft or violent crime.
Other economic costs

In addition to these economic costs of crime, society may also suffer economic loss due to sick days taken by and low productivity of employees using drugs. The business sector, in addition to governments, may suffer significant costs on account of illicit drug use.61

Smith et al., when considering the costs of illicit drug use to society in 2011, estimated the costs of lost productivity of those in hospital or treatment related to illicit drug use as being $425 million.62 They also estimated the costs attributable to illicit drug use deaths, which they estimated to be 974 in 2011 at a rate of $2.12 billion, including lost productivity and medical costs.63

Some other costs to the community include the costs incurred by the Department of Communities, Child Safety and Disability Services in ensuring that children of drug users who have suffered neglect or abuse are appropriately cared for, and costs of welfare reliance caused by drug abuse.

Risk of safety to the community

Another way in which the community is affected by illicit drug use is through risks to the safety of individuals that are posed by people using and producing illicit drugs.

Frontline workers such as police officers, medical staff and social workers are at particular risk of being the victim of a violent offence due to their exposure to persons under the influence of illicit drugs.

A 2008 study of methylamphetamine and heroin users in Sydney found that 18 per cent of heavy methylamphetamine users had violently attacked a police officer in their lifetime, with 19 per cent of persons who heavily used both methylamphetamine and heroin admitting to attacking a police officer in the past. For heavy heroin users, 15 per cent had attacked a police officer in their lifetime.64

The wider community can also be at risk from drug-related behaviour. In the National Drug Strategy Household Survey in 2013, 8.3 per cent of the population reported that they had been a victim of an incident related to illicit drugs.65 The proportion of those that were the victim of a violent drug-related incident rose from 2.2 per cent in 2010 to 3.1 per cent in 2013.66

In addition to the risk of physical violence, there is also a risk of injury due to accidents caused by people under the influence of drugs.

Drugs can affect a person’s neurological functions, their perception, attention, cognition, coordination and reaction time,67 which can put others at risk on the roads when people choose to drive after consuming drugs.

There are differing estimates about the role of ‘drug driving’ in traffic accidents in Australia. Some studies have estimated that drug driving is a contributing factor in approximately seven per cent of road fatalities in Australia.68 That figure does not include instances where drugs were used in conjunction with alcohol.69

In New South Wales, 195 deaths were attributed to drug driving in the period between 2010 and 2013 by Transport for New South Wales, accounting for approximately 13 per cent of the road toll.70 One hundred and seventy four drivers with at least one of three illicit drugs (cannabis, methylamphetamine or MDMA/‘ecstasy’) in their system were involved in these accidents. Thirty-four of these were motorbike riders and 20 were heavy truck drivers.71

Despite the differing estimates, it is clear that driving under the influence of drugs contributes, to some extent, to traffic accidents—including fatal accidents. In the 2013 National Drug Strategy Household Survey, 15.9 per cent of recent illicit drug users reported they had driven a vehicle while under the influence of illicit drugs in the past 12 months.72
The Commission issued a notice to the QPS to provide statistics in relation to the number of road users tested by police for being under the influence of drugs during the period of 1 July 2014 – 30 June 2015. The Deputy Commissioner advised in a sworn statement to the Commission that 20,389 tests were conducted under the roadside drug testing program in this period. Of those tested, the number who tested positive for the prevalence of a relevant drug was 2,168 drivers. The QPS is awaiting analysis results for 1,003 drivers. Of note, the current testing regime only provides for the testing of methamphetamine, MDMA/‘ecstasy’ and cannabis. Accordingly, this would not capture that portion of the population under the influence of a drug analogue or new psychoactive substance. Recently, there were reports that one in five drivers tested positive for drug driving in Queensland over the June 2015 Queen’s birthday long weekend.

These figures are extremely concerning, given the effects of drug use on the driver and the risk of serious injury or death to both the drug user and to innocent people on the roads.

The effect of drug use on driving is transferable to the operation of heavy machinery. The National Drug Strategy Household Survey 2013 reported that 10.4 per cent of recent drug users had attended work under the influence of illicit drugs in the 12 months prior to the survey, and 3.6 per cent admitted to operating a boat or hazardous machinery. In workplaces where the use of heavy machinery is common, employees under the influence of drugs put both themselves and their workmates at risk of accident or injury.

Even in workplaces where heavy machinery is not present, the effects of drugs may pose a risk to the health and safety of others. For example, the effects of drugs and alcohol by those in the medical profession—such as nurses—could lead to impaired judgment and decision-making, mismanagement of medication, unsafe practices, and negligence. This could present a risk of harm to patients, in addition to co-workers.

The safety of the community generally can also be affected by illicit drugs through the establishment of clandestine drug laboratories in residential and business areas. The Australian Crime Commission (ACC) reported that in 2013–2014, there were 744 clandestine drug laboratories detected across Australia, with residential areas being the main location in which they were detected. Queensland had the highest proportion of laboratory detections, accounting for 45.8 per cent of detections. The Australian Crime Commission figures show that Queensland has consistently had the highest number of detections for the past decade.

In Queensland, the majority of laboratories produced amphetamine type-stimulants, not including MDMA/‘ecstasy’.
Clandestine drug laboratories are clearly an issue for residents of Queensland. These laboratories pose a risk because the precursor chemicals used to make drugs are often corrosive, toxic or highly flammable. Although gas or aerosol contamination from clandestine laboratories usually remains in the surrounding area or dilutes when they disperse, fire or explosion can still be a risk to residents in the vicinity.

Those who subsequently move into a property where the chemicals from a clandestine laboratory have not been adequately cleaned may suffer adverse health consequences from residual chemical contamination absorbed by floorings, walls, drains and furnishings.

Frontline workers such as police officers and fire fighters may also be exposed to risks when investigating or responding to incidents at these sites.

In addition to affecting occupants and neighbours, clandestine drug laboratories also pose a risk to the environment. In many instances, waste is dumped on public lands, in sewerage systems, at industrial estates, and in national parks and waterways, contaminating those sites with hazardous chemicals.

3.3.2 Conclusion

It is clear that illicit drug use can have tragic consequences for users. However, it is also clear that drug use touches on the broader community—whether that be through the allocation of tax revenue to drug-related health, welfare and criminal justice issues, through the diversion of hospital beds, through a loss of productivity in the workforce, through property theft or violent crime, or as a result of road- or work-related accidents. The financial and social costs to the community are great, and when one considers the impacts of a drug upon a person, consideration should also be given to the significant financial and social impacts that these drugs have upon our society as a whole.

(Endnotes)


The illicit drug market


3 The illicit drug market


73 Statutory Declaration of Ross Barnett, 17July 2015 [In-Confidence].

3.4 Legislation

The Commission was required to investigate and evaluate the adequacy of current legislation available to law enforcement, criminal intelligence, and prosecution agencies in Queensland to prevent and effectively investigate and prosecute organised criminal activity. In terms of the drug market in Queensland, there are a number of pieces of legislation that are relevant and need to be considered.

At a state level, the relevant legislation concerning drug offences are the *Drugs Misuse Act 1986* and the *Drugs Misuse Regulation 1987*. The *Police Powers and Responsibilities Act 2000* is the relevant legislation to consider in terms of police powers in relation to drug offences. At a Commonwealth level, the legislation to consider is the *Criminal Code Act 1995*, and in relation to the powers of federal agents, the *Crimes Act 1914*.

3.4.1 Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987

The Drugs Misuse Act provides the offences and penalties associated with illicit drugs in Queensland. This section of the report focuses on the four main offence provisions within the Act: possessing, supplying, producing and trafficking in dangerous drugs.

The Drugs Misuse Act works in conjunction with the Drugs Misuse Regulation. The term ‘dangerous drug’ is defined in section 4 of the Drugs Misuse Act as meaning a substance specified in Schedules 1 or 2 of...
the Drugs Misuse Regulation, and extends to analogues, salts, derivatives and stereo-isomers of such Scheduled substances.

The offence provisions in the Drugs Misuse Act contain tiered maximum penalties. For the offence of trafficking in dangerous drugs, the relevant maximum penalty is dependent on the type of drug trafficked. For the offence of supplying dangerous drugs, the relevant maximum penalty is dependent on the type of drug supplied and the circumstances of the supply. For example, supplying to a minor or within a correctional facility attracts a higher maximum penalty. The relevant maximum penalties for the offences of producing and possessing dangerous drugs are dependent on the type and quantity of drug produced or possessed.

It is clear that the legislature considers certain illicit drugs as more serious than others.

Substances listed in Schedule 1 of the Drugs Misuse Regulation attract the higher maximum penalties and are therefore considered the most serious by the legislature. The drugs listed in Schedule 1 are amphetamine, cocaine, heroin, lysergide, methylamphetamine, 3,4-Methylenedioxymethamphetamine (MDMA), paramethoxymphetamine (PMA), paramethoxymethamphetamine (PMMA), and phencyclidine.

Part 2 of Schedule 1 was inserted into the Schedule in 2014 and, in effect, transferred all the steroids out of Schedule 2 and into Schedule 1.

Schedule 2 contains the remaining dangerous drugs. Some of the dangerous drugs located within Schedule 2 include cannabis, synthetic cannabis, 3,4-methylenedioxypyrovalerone (MDPV), fentanyl, and many of the drug analogues discussed earlier in the report, with the exception of PMA and PMMA, which are Schedule 1 drugs.

Schedule 3 specifies quantities for all the drugs listed in Schedules 1 and 2. Schedule 4 provides further quantities for the Schedule 1 drugs.

Therefore, determining the relevant maximum penalty for a person charged with possessing or producing a dangerous drug involves a two-stage process: first, determining whether the substance is proscribed in either Schedule 1 or Schedule 2 of the Drugs Misuse Regulation, and second, referring to Schedules 3 and 4 (in the case of a Schedule 1 drug) to consider the specified quantities. For the offences of possessing and supplying a dangerous drug, the determination of the relevant maximum penalty becomes even more complex as those provisions list a number of aggravating circumstances.

The tiered maximum penalties for the offence of possessing a dangerous drug are located within the offence section. If the drug is a Schedule 1 drug and the quantity is or exceeds the amount specified in Schedule 4, then the maximum penalty is 25 years imprisonment. If the quantity involved is or exceeds the quantity in Schedule 3 but is less than Schedule 4 and the person was a drug-dependent person at the time of the offence, then the maximum penalty is 20 years imprisonment. If the quantity is of or exceeds the quantity in Schedule 3 but is less than Schedule 4 but the person was not a drug-dependent person, then the maximum penalty is 25 years imprisonment. If the drug is a Schedule 2 drug and the quantity is or exceeds the quantity specified in Schedule 3 then the maximum penalty is 20 years imprisonment. In any other case, whether the drug be Schedule 1 or 2 the maximum penalty is 15 years imprisonment.

The tiered maximum penalties for the offence of producing a dangerous drug are located within the offence section. If the drug is a Schedule 1 drug and the quantity is or exceeds the amount specified in Schedule 4 then the maximum penalty is 25 years imprisonment. If the quantity involved is or exceeds the quantity in Schedule 3 but is less than Schedule 4 and the person was a drug-dependent person at the time of the offence then the maximum penalty is 20 years imprisonment. If the quantity is of or exceeds the quantity in Schedule 3 but is less than Schedule 4 but the person was not a drug-dependent person then the maximum penalty is 25 years imprisonment. In any other case where the drug is a Schedule 1 drug, the maximum penalty is 20 years imprisonment. If the drug is a Schedule 2 drug and the quantity is or exceeds the quantity specified in Schedule 3, then the maximum penalty is 20 years imprisonment. In any other case with a Schedule 2 drug the maximum penalty is 15 years imprisonment.
Again, there is a clear distinction between Schedule 1 and Schedule 2 drugs with this offence and the associated penalties.

The tiered maximum penalties for the offence of supplying a dangerous drug are located within the offence section. If the drug is a Schedule 1 drug and there is a circumstance of aggravation in that the person supplied the drug to a minor under the age of 16 years, then the maximum penalty is life imprisonment.\(^\text{14}\) If the drug is a Schedule 1 drug and there is a circumstance of aggravation in that the person to whom the thing supplied to is a minor who is 16 years or more, an intellectually impaired person, is within an educational institution, is within a correctional facility or if the person does not know they are being supplied with the thing, then the maximum penalty is 25 years imprisonment.\(^\text{15}\) In any other case with a Schedule 1 drug the maximum penalty is 20 years imprisonment.\(^\text{16}\) A similar scheme is applied to Schedule 2 drugs with the maximum penalties for the offences being 25 years imprisonment, 20 years imprisonment and 15 years imprisonment respectively.\(^\text{17}\)

The penalties for the offence of trafficking in a dangerous drug are located within the offence section. If the drug is a Schedule 1 drug then the maximum penalty is 25 years imprisonment.\(^\text{18}\) If the drug is a Schedule 2 drug then the maximum penalty is 20 years imprisonment.\(^\text{19}\) When sentencing a person for trafficking in a dangerous drug, the court must order that the person serve a minimum non-parole period of 80 per cent of the term of imprisonment imposed.\(^\text{20}\) The mandatory minimum non-parole period does not apply if the person is sentenced to either an intensive correction order or a suspended sentence.\(^\text{21}\)

It is evident from the penalty structure provided in the Drugs Misuse Act that the legislature views the Schedule 1 drugs as more serious than those substances listed in Schedule 2, and that persons possessing or supplying Schedule 1 drugs should be liable to greater maximum penalties. However, this approach is difficult to reconcile when considering the upgrade of steroids to Schedule 1 and inconsistencies between the Schedules, such as PMA and PMMA being listed as Schedule 1 drugs while other synthetic psychoactive substances are listed in Schedule 2. The approach also injects a complexity into the penalty regime and it is not readily transparent and discernable as to the relevant maximum penalties.

It is of interest to note that that with the exception of the Northern Territory, no other Australian jurisdiction has a classification system like the one in existence in Queensland where different dangerous drugs are treated more seriously than others, with regard to maximum penalties imposed. The Commission has had particular regard to the legislative schemes in place in New South Wales and Victoria.

**Jurisdictional comparison**

**New South Wales**

In New South Wales, the *Drug Misuse and Trafficking Act 1985* and *Drug Misuse and Trafficking Regulation 2011* are the two relevant pieces of legislation dealing with dangerous drugs. The Drugs Misuse and Trafficking Act has one schedule which lists all prohibited plants and drugs. The legislation does not differentiate between the drugs. The schedule has a number of columns prescribing different weights to different categories. The categories included in the Act are as follows:

- Traffickable quantity (column 1)
- Small quantity (column 2)
- Indictable quantity (column 3)
- Commercial quantity (column 4)
- Large commercial quantity (column 5)
- Discrete dosage unit (column 6)

The order of quantity is from small quantity, to traffickable quantity, indictable quantity, commercial quantity and then large commercial quantity. The final column relating to discrete dosage unit is not relevant for present purposes.
To illustrate, a selection of drugs from schedule 1 of the New South Wales Act is included below.

<table>
<thead>
<tr>
<th>Prohibited plant or drug</th>
<th>Traffickable quantity</th>
<th>Small quantity</th>
<th>Indictable quantity</th>
<th>Commercial quantity</th>
<th>Large commercial quantity</th>
<th>Discrete dosage unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heroin</td>
<td>3.0 g</td>
<td>1.0 g</td>
<td>5.0 g</td>
<td>250 g</td>
<td>1.0 kg</td>
<td>-</td>
</tr>
<tr>
<td>Cocaine</td>
<td>3.0 g</td>
<td>1.0 g</td>
<td>5.0 g</td>
<td>250 g</td>
<td>1.0 kg</td>
<td>-</td>
</tr>
<tr>
<td>MDMA</td>
<td>15 DDU or 3.0 g</td>
<td>4 DDU or 0.8 g</td>
<td>25 DDU or 5.0 g</td>
<td>0.5 kg</td>
<td>2.0 kg</td>
<td>0.2 g</td>
</tr>
<tr>
<td>Methylamphetamine</td>
<td>3.0 g</td>
<td>1.0 g</td>
<td>5.0 g</td>
<td>250 g</td>
<td>1.0 kg</td>
<td>-</td>
</tr>
<tr>
<td>Cannabis leaf</td>
<td>300.0 g</td>
<td>30.0 g</td>
<td>1 kg</td>
<td>25 kg</td>
<td>100 kg</td>
<td>-</td>
</tr>
<tr>
<td>MDPV</td>
<td>3.0 g</td>
<td>1.0 g</td>
<td>5.0 g</td>
<td>500.0 g</td>
<td>2.0 kg</td>
<td>-</td>
</tr>
<tr>
<td>PMA</td>
<td>15 DDU or 3.0 g</td>
<td>4 DDU or 0.8 g</td>
<td>25 DDU or 5.0 g</td>
<td>0.25 kg</td>
<td>1.0 kg</td>
<td>0.2 g</td>
</tr>
</tbody>
</table>

As can be seen from this selection of drugs from Schedule 1, the drugs have different quantities assigned to each category. It is the category that determines the jurisdiction of the matter as well as the penalty applicable to the offences.

Possessing a prohibited drug is an offence under section 10 of the Drugs Misuse and Trafficking Act. Pursuant to section 9 of the Act, the offence is a summary offence which must be disposed of in the Local Court (which is equivalent to the Magistrates Courts in Queensland). Section 29 of the Act is a deeming provision which provides that a person in possession of a traffickable quantity (or more) of a prohibited drug is deemed to possess the drug for the purpose of supplying it, unless the person proves to the contrary. Therefore, a person in possession of a traffickable quantity of a prohibited drug will be charged with the offence of supplying a dangerous drug which is an offence under section 25 of the Act. It is worth noting that prohibited plants are dealt with in a separate offence (section 23 of the Act).

The offences of producing and supplying prohibited drugs and the offences of cultivating, supplying and possessing prohibited plants are indictable offences. Sections 30 and 31 of the Drugs Misuse and Trafficking Act allow for the summary disposition of indictable offences at the election of the prosecution in the case of small quantities and at the election of the prosecution or defence in the case of quantities that do not exceed the indictable quantity. Indictable offences dealt with summarily are liable to a maximum jail term of two years imprisonment. Aggravated supply to a child under 16 years carries two years and six months.

The fact that New South Wales does not distinguish between their prohibited drugs in terms of maximum penalties arguably makes for a simpler penalty regime than in Queensland. For example, under New South Wales laws, a conviction for possessing a prohibited drug carries a maximum penalty of 20 penalty units and/or two years imprisonment (noting that possessing a traffickable quantity is deemed a supply with the onus on the defendant to prove to the contrary). The offences of cultivating, supplying and possessing prohibited plants and supplying and producing prohibited drugs, not involving commercial quantities and with no other circumstance of aggravation, carry maximum penalties of 2000 penalty units and/or 15 years imprisonment; except for cannabis which carries a maximum penalty of 2000 penalty units and/or 10 years imprisonment.

The above non-exhaustive outline of the offence and penalty provisions in New South Wales provides a useful comparison to Queensland’s offence/penalty regimes. In New South Wales, with the exception of cannabis which has lower maximum penalties than other prohibited drugs in some circumstances, it is the...
offence that deems the maximum penalty to be applied and not the type of drug. For example, there is no differentiation between methylamphetamine (a Schedule 1 drug in Queensland) and MDPV (a Schedule 2 drug in Queensland) as both are prescribed the same penalties. In New South Wales, the relevant maximum penalty depends on the offending conduct and the quantity of the drug involved.

**Victoria**

In Victoria, the Drugs, Poisons and Controlled Substances Act 1981 (Vic) deals with dangerous drugs. In Victoria, these drugs are referred to as ‘drugs of dependence’ and all such drugs are listed in Schedule 11 of the Act. There are three parts to Schedule 11; however, for the purpose of offence and penalty provisions it does not matter what part the drugs fall into. Parts 2 and 3 of the Schedule contain the drugs of dependence of most relevance and under these parts there are a number of columns prescribing different weights to different categories. The main categories are:

- Large commercial quantity
- Commercial quantity
- Traffickable quantity
- Small quantity

Possessing a drug of dependence is an offence under section 73 of the Drugs, Poisons and Controlled Substances Act. The penalties for that offence are located within the section. If the possession relates to a quantity not greater than the small amount of cannabis, then the penalty is five penalty units. If it is any other drug and the court is satisfied that the possession was not for the purpose of trafficking then the maximum is 30 penalty units and/or one year imprisonment. In any other case the penalty is a maximum of 400 penalty units and/or five years imprisonment. Section 73(2) provides that a traffickable quantity is prima facie evidence that the possession is for the purpose of trafficking.

Trafficking in a dangerous drug is an offence under section 71AC of the Drugs, Poisons and Controlled Substances Act. Sections 71, 71AA and 71AB provide for aggravated trafficking offences of trafficking in large commercial quantities, in commercial quantities and to a child, respectively.

Section 70 of the Act defines traffick to include:

(a) Prepare a drug of dependence for trafficking;
(b) Manufacture a drug of dependence; or
(c) Sell, exchange, agree to sell, offer for sale or have in possession for sale, a drug of dependence.

Accordingly, there are no general offences of producing or supplying a dangerous drug, as such conduct is captured under the definition of trafficking. There is a discreet offence of supplying to a child and offences dealing with the cultivation of narcotic plants.

With regards to the offences of trafficking, the maximum penalties are not dependant on the type of drug involved, but rather hinge on the quantity of drug (under a commercial quantity, a commercial quantity or a large commercial quantity) or the circumstance of aggravation of supplying to a child.

**Commonwealth**

The Commonwealth’s Criminal Code Act 1995 and the Criminal Code Regulation 2002 provide the illicit drug laws for the Commonwealth. The Regulation contains two schedules outlining controlled and border controlled drugs. There is no distinction in the schedules between different types of drugs. For example, cannabis, cocaine, MDPV and heroin are all listed on both schedules. There are columns within the schedules specifying the commercial quantity, marketable quantity and trafficable quantity for controlled drugs, and the commercial quantity and marketable quantity for border controlled drugs. Accordingly, the Commonwealth operates a similar system to New South Wales and Victoria whereby all drugs are on the one schedule, and that same schedule outlines the quantities applicable to various circumstances of aggravation.
By way of example, trafficking in a dangerous drug is proscribed in sections 302.2 – 302.4 of the Criminal Code Act, with the different sections relating to different quantities of drugs. The penalties for the offences are also found within that section. Regardless of the drug involved, the person is liable to the same maximum penalty. The criminality lies in the offence and the quantity of drugs involved, not in the drug type.

A need for a simpler regime in Queensland?

The illicit drugs market is inextricably linked to organised crime. Australian states and territories have a long and extensive list of laws designed to promote general and personal deterrence and reduce the number of drug offences committed. Despite such laws, the illicit drug market remains highly lucrative, with the demand for a wide variety of drugs growing. Further, Queensland remains in a period of growth within the drug market, particularly in respect of amphetamine-type stimulants, cannabis and steroids.

One of the main points of difference between the legislative schemes is the way in which substances are classified and grouped. Queensland has arguably the most complex classification system, with substances spread across six separate schedules. Substances classified as dangerous drugs are divided between two schedules which must be read in conjunction with two further schedules before maximum penalties—and therefore jurisdiction—can be established. This approach produces a penalty regime which is not readily discernable to the public, a circumstance that may detract from the deterrence value of Queensland’s scheme.

With reference to the penalties, drugs contained in Schedule 1 are deemed more serious than those contained in Schedule 2. This approach is difficult to reconcile when considering the upgrade of steroids to Schedule 1, and inconsistencies between the Schedules, such as PMA and PMMA being listed as Schedule 1 drugs while other synthetic psychoactive substances are listed in Schedule 2.

With the exception of the Northern Territory, no other state or territory in Australia has a classification system whereby different dangerous drugs are treated as more serious than others, having regard to the maximum penalties applicable for offences.

It is therefore necessary to discuss the way in which drugs reach the different schedules in Queensland to consider the efficiency and effectiveness of this process.

The process for listing a substance: How drugs reach a schedule in Queensland

Before a Minister makes a recommendation to the Executive Council to have a substance placed into a schedule of the Drugs Misuse Regulation, the Minister is statutorily bound to consider certain matters.

Section 134A of the Drugs Misuse Act provides as follows:

1. In deciding whether to recommend the prescription of a thing as a dangerous drug for the Drugs Misuse Regulation 1987, Schedules 1 to 5, the Minister must consider the following—
   a. the likelihood or evidence of abuse of the drug, including, for example, the prevalence of the drug, consumption levels of the drug, the potential appeal of the drug to vulnerable populations and drug seizure trends;
   b. specific effects of the drug, including, for example, the pharmacological, psychoactive and toxicological effects;
   c. the risks, if any, of the drug to public health and safety;
   d. the therapeutic value, if any, of the drug;
   e. the potential for use of the drug to cause death;
   f. the ability of the drug to create physical or psychological dependence;
   g. the classification and experience of the drug in other jurisdictions;
   h. any other matters the Minister considers appropriate.

2. However, the Minister may decide to recommend the prescription of a thing without complying with subsection (1) if the Minister is satisfied it is necessary to recommend the prescription of the thing as a matter of urgency having regard to 1 or more of the matters listed in subsection (1).
In responding to a notice issued by the Commission, Mr David Mackie, Director-General of the Department of Justice and Attorney-General (DJAG), provided information about the process that applies to ensure the Minister is appropriately briefed and able to consider the matters listed in section 134A.

There is a standing inter-departmental working group (IDWG) which is chaired by DJAG and which meets to identify deficiencies in the Drugs Misuse Act and Drugs Misuse Regulation. The IDWG does not directly advise the Attorney-General; however, officers from the Strategic Policy unit in DJAG, who are part of the working group, provide this advice. Membership of the IDWG includes officers from the Strategic Policy unit of DJAG, the Department of the Premier and Cabinet, Queensland Health and the Queensland Police Service (QPS) Drug Squad. The IDWG does not appear to have uniform meeting times, but meets at least twice per year. Mr Mackie advised that generally the process of scheduling a drug begins after advice is received from the QPS about a particular substance warranting classification. In addition to this, Mr Mackie advises that the development of drug policy reform in Queensland is informed by a range of other sources.

Detective Inspector Mark Slater of the QPS Drug Squad, in his interview with the Commission, provided some insight into the process of having a drug placed into a Drugs Misuse Regulation Schedule, based on his experience. He advised that the process itself in arranging a meeting with the IDWG was not difficult, but the real challenge lay with the research that needs to be completed to show the harm associated with the drug, before a recommendation can be made to have it reach the appropriate schedule. When questioned as to the main consideration as to which schedule it is recommended to be placed in, Detective Inspector Slater advised that the impact on society and the harm factor were the key considerations when determining which schedule it should be recommended to be placed in.

A consideration of Schedules 1 and 2 reveals that it is not readily apparent why one drug is placed in Schedule 1 and another may be placed in Schedule 2. The Commission understands that there are a number of drugs listed in Schedule 2 which have been responsible for a number of deaths both in Australia and overseas. The quantities of these drugs that need to be digested to have a fatal effect can in some cases be considerably smaller than those drugs which are classified as Schedule 1 drugs. For example, the Schedule 2 drug fentanyl is an opioid analgesic that authorities estimate to be between 80 to 100 times more potent than morphine. The drug is normally prescribed to treat cancer patients, but when misused has effects similar to heroin, a Schedule 1 drug. The Crime and Corruption Commission (CCC) have noted that there have been more fatal overdoses associated with fentanyl in Queensland than in any other State of Australia.

In response to a notice issued by the Commission, Mr Mackie provided copies of all briefs and attachments submitted to the Minister regarding drug schedules in the Drugs Misuse Regulation for the period 1 January 2012 to the date of the notice, May 2015. An examination of the material provides insight into the type of information provided to the Minister by the Department. The brief dealing with the proposed scheduling of the drugs MDPV and PMMA is of interest, as the result of the process was the listing MDPV in Schedule 2 and PMMA into Schedule 1.

On 27 November 2012, a brief for decision was provided to the then-Attorney-General and Minister for Justice from the Strategic Policy unit in DJAG. The brief contained recommendations for a number of substances to be classified as dangerous drugs and placed into either Schedule 1 or Schedule 2 of the Drugs Misuse Regulation. The information in the brief addressed those relevant considerations outlined in section 134A of the Drugs Misuse Act.

One of the drugs contained in the recommendation was methylenedioxyprovalerone (MDPV). It was recommended that MDPV be classified as a Schedule 2 dangerous drug. The following was contained within an attachment to the brief.
During late 2010 and 2011 the emergence of MDPV in suspected illicit drug seizures increased. Queensland reported the frequency of MDPV detections increased from 18 items in 2010 to 80 items in 2011 and the significant increases in seizures of MDPV from 2010 (eight seizures) to 2011 (63 seizures).

A search of the internet revealed a number of Australian and overseas sites that offer MDPV for sale.

In an attempt to circumvent legislation, MDPV is marketed as a legal alternative to illicit drugs and has been named by social networking groups as synthetic cocaine. In 2009 a consignment of MDPV was intercepted by Australian Customs Service and investigated by the State Drug Investigation Unit. The consignment was labelled as ‘bath salts’ and was destined for distribution throughout Queensland and other States.

MDPV is a psychoactive drug with stimulant properties. MDPV is a chemical analogue of pyrovalerone which is a Schedule 2 dangerous drug in the Drugs Misuse Regulation.

It is believed that very small doses of MDPV are very potent, which contrasts significantly even with drugs such as heroin.

MDPV acts as a stimulant. According to the Drug Enforcement Administration (DEA)(USA): “MDPV has been reported to induce subjective effects in humans similar to those induced by cocaine amphetamine and MDMA. The subjective effects induced by substituted cathinones are feelings of empathy, stimulation, alertness, euphoria, and awareness of senses. Other effects reported from the use of MDPV were prolonged panic attacks in users. Repeat users have reported bouts of psychosis and a craving or a strong desire or urge to use again. Users of MDPV anecdotally reported that they take 25mg or less per session. The duration of the subjective effects is about two to three hours whereas the adverse effects have been reported lasting six to eight hours after administration.”

High doses have been observed to cause intense, prolonged panic attacks in stimulant-intolerant users, and there are anecdotal reports of psychosis from sleep withdrawal and addiction at higher doses or more frequent dosing intervals.
### The risk, if any, of the drug to public health and safety.

MDPV related deaths have been reported in the USA and UK as a result of overdose and fatal injuries as a result of high levels of intoxication and psychosis.

Advice has been received from South Australian State Intelligence Branch that MDPV has been reported to be linked to a number of hospital presentations for non-fatal overdoses and at least one overdose-related death.

In April 2011, in Illinois USA, a woman apparently died from an MDPV overdose.

In May 2011, the Centres for Disease Control and Prevention (USA) reported a hospital emergency department visit after the use of ‘bath salts’ in Michigan. One person was reported dead on arrival at the emergency department. Associates of the dead person reported that he had used bath salts. His toxicology results revealed high levels of MDPV in addition to marijuana and prescription drugs. The primary factor contributing to death was cited as MDPV toxicity after autopsy was performed.

MDPV is known to be popular in the mining industry as it is not easily detectably in drug testing and this is supported by a Queensland Police Service (QPS) report outlining significant availability and use of the drug in the mining town of Mount Isa.

### The therapeutic value, if any, of the drug.

No therapeutic use, although has been used in the past as nasal decongestant.

### The potential for use of the drug to cause death.

See above entry for 134A(c).

### The ability of the drug to create physical or psychological dependence.

As stated above, the DEA reports “Repeat users have reported bouts of psychosis and a craving or a strong desire or urge to use again”.

### The classification and experience of the drug in other jurisdictions.

**Western Australia:** MDPV has been banned under the *Poisons Act 1964* since 11 February 2012.

**Australia:** The Therapeutic Goods Administration has included MDPV in the *Standard for the Uniform Scheduling of Medicines and Poisons* (the Poisons Standard).

**Canada:** Listed in Schedule 1 of the *Controlled Drugs and Substances Act* since 5 June 2012.

**USA (Federal):** on 21 October 2011 the DEA issued a one year, Schedule 1, ban on MDPV. Schedule 1 status is reserved for those substances with a high potential for abuse, no currently accepted use for treatment in the USA and a lack of accepted safety for use of the drug under medical supervision.

**USA (States):** Banned in at least seven States.

**UK:** Controlled since April 2010.
Within the same brief was a recommendation that the drug paramethoxymethamphetamine (PMMA) be listed as a Schedule 1 dangerous drug. The following information was contained in an attachment to the brief.

| The likelihood or evidence of abuse of the drug including, for example, the prevalence of the drug, consumption levels of the drug, the potential appeal of the drug to vulnerable populations and drug seizure trends. | Paramethoxymethamphetamine also known as PMMA was first seized by the Queensland Police Service (QPS) in 2008. Queensland Health Forensic and Scientific Services (QHFSS) first analysed PMMA in 2009. PMMA has been seized by QPS and analysed by QHFSS every year since 2008. In 2012 there has been a rise in the number and weight of PMMA detections. In September 2012, the South Australian Police advised that they seized a quantity of precursor chemicals which were intended to be used to produce PMMA. |
| The specific effects of the drug, including, for example, the pharmacological, psychoactive and toxicological effects. | PMMA is a derivative of paramethoxyamphetamine (PMA) which is a dangerous drug under Schedule 1 Drugs Misuse Regulation 1987. It is a stimulant and psychedelic drug. It is sold as tablets for oral consumption. PMMA has been found in tablets and capsules for MDMA (Schedule 1 drug) sold as ‘ecstasy’. It has similar effects as MDMA but with increased toxicity. |
| The risk, if any, of the drug to public health and safety. | The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) reported on PMMA. The EMCDDA reports that: ‘PMMA is taken in the context of an ‘ecstasy’ culture in which prior expectations exist with regard to the quality and the timing of the effects. Consequently, the poor MDMA-like effects of PMMA, even when combined with PMA, may be perceived as a weakness or a failure of the pill taken in the belief that it is ‘ecstasy’. This may lead to the consumption of more pills and subsequent overdose.’ The drug user website erowid reports: ‘PMMA is a strong stimulant that may cause dangerous overheating of the body. It has been detected in ecstasy tablets since the early 1990s, and has led to life threatening or fatal hyperthermia in some users.’ |
| The therapeutic value, if any, of the drug. | No therapeutic value. |
| The potential for use of the drug to cause death. | The QPS are currently investigating a number of fatal overdoses involving PMMA. Two of these instances are believed to be directly related to PMMA however investigations have not been finalised. Internationally, a number of deaths have been attributed to PMMA, including in Norway and Scotland. In January 2012, a number of ecstasy related deaths in Canada in the previous year were linked to PMMA overdoses. It is upon the basis of the deaths from PMMA that it is recommended to be included in Schedule 1 rather than Schedule 2. |
The illicit drug market

The ability of the drug to create physical or psychological dependence.

<table>
<thead>
<tr>
<th></th>
<th>The EMCDDA report states:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dependence</td>
</tr>
<tr>
<td></td>
<td>Drug discrimination learning for PMMA has only been studied in animals. Low doses of PMMA (1.25mg/kg) have a discriminative stimulus similar to that induced by ‘entactogen’ substances such as MDMA. There have been no systematic studies of the potential for PMMA dependence in animals or humans. The lack of dopamine effects would tend to indicate a low dependence potential because of the central reinforcing role of dopamine release. In contrast with MDMA effects, reports from users indicate reduced motivation to talk and to get involved with others, and undesired physical effects. It is unlikely that, in the long term, fake ‘ecstasy’ tablets combining PMMA and PMA could replace MDMA on the retail market.</td>
</tr>
</tbody>
</table>

The classification and experience of the drug in other jurisdictions.

<table>
<thead>
<tr>
<th></th>
<th>PMMA is controlled in EU member states. UK: Illegal as a Class A drug.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A further amendment to the Schedules worth noting is the 2014 reclassification of anabolic steroids from a Schedule 2 drug to a Schedule 1 drug. The reclassification resulted in increased maximum penalties for unlawfully possessing and supplying anabolic steroids, but the evidence base behind the reclassification is questionable.

The Newman Government introduced the reclassification of steroids as part of the Safe Night Out Legislation Amendment Act 2014, an Act introduced into the Legislative Assembly in June 2014 and aimed at reducing alcohol and drug-related violence in Queensland’s nightlife. The Explanatory Notes to the Act and the then-Premier’s Introduction speech offer no insight into the rationale behind the reclassification other than to observe that the strengthened maximum penalties will be similar to those applying to dangerous drugs such as methamphetamine and ecstasy. The then-Premier was reported in a number of media articles linking outlaw motorcycle gangs with gyms and the trafficking and supply of steroids.

Given that the reclassification of steroids occurred by an amending Act rather than by an amending regulation, section 134A of the Drugs Misuse Act did not strictly need to be complied with. However, in the interests of transparency, Strategic Policy, DJAG provided the then Attorney-General with relevant information by way of a brief dated 11 June 2014. An extract from the information provided is outlined below and includes information from Queensland Health that the major public health issue relating to steroid use centres around increased cardiovascular disease. Risks in terms of violent behaviour have not been studied in any prospective way. While aggression and violence associated with illicit steroid use is likely to exist, the limited studies that exist do not identify a specific predictive factor as to which individuals will become aggressive. The information does not refer to steroids as a drug commonly found in the ‘club scene’ (unlike methamphetamine and ecstasy). The Commission queries whether such evidence supported rescheduling steroids to Schedule 1 and is offered as another example of inconsistencies that occur with the two Schedule regime.

The following information was contained in an attachment to the brief.
The likelihood or evidence of abuse of the drug including, for example, the prevalence of the drug, consumption levels of the drug, the potential appeal of the drug to vulnerable populations and drug seizure trends.

The Queensland Police Service (QPS) advises that Performance and Image Enhancing Drugs (PIEDs) (which includes steroids) are often seized ancillary to investigations involving other drugs (such as cocaine or amphetamine type stimulants) or where specific intelligence identifies organised criminality around the trafficking and supply of PIEDs.

Qld Seizure Data

<table>
<thead>
<tr>
<th></th>
<th>2010-2011</th>
<th>2011-2012</th>
<th>2012-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seizures</td>
<td>16</td>
<td>28</td>
<td>46</td>
</tr>
<tr>
<td>Weight (kg)</td>
<td>1.43</td>
<td>0.216</td>
<td>4.00</td>
</tr>
</tbody>
</table>

Arrest Data

<table>
<thead>
<tr>
<th></th>
<th>2010-2011</th>
<th>2011-2012</th>
<th>2012-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrests</td>
<td>231</td>
<td>296</td>
<td>392</td>
</tr>
</tbody>
</table>

2011-2012 border seizures indicate that there were 6126 steroid seizures by Australian Customs.

91.5% of these seizures were made through the parcel post.

Nationally in 2011-2012, steroid seizures and arrest numbers were the highest on record.

There is no current intelligence suggesting PIEDs are manufactured in clandestine drug laboratories in Queensland.

PIEDs are generally imported in raw powder form then mixed with other preparations for the purpose of administration. These PIED mixing labs represent a relatively low risk in comparison with other clandestine labs such as methamphetamine or MDMA as there is no chemical synthesis or processes involved, the chemicals are relatively stable and are not considered hazardous. Kitchen utensils are the only equipment used in the mixing process. The chemicals used in the mixing process are not controlled under precursor control legislation and most have wide ranging legitimate uses in industry and the wider community.

Recent intelligence from certain chemical suppliers in the Brisbane metropolitan area has identified an increasing number of purchases of the chemicals used in the mixing process with raw PIEDs.

Queensland Health (QH) advises that data on the pattern of steroid use in the Needle and Syringe Programs show that there has been an increase in the number of service occasions related to steroid use across the programs for most age groups with it being greater in the 19-24 year age group. Most of the service occasions are for male clients. On the data, overall steroid use has more than tripled (2.6% to 8.1%) between 2008 and 2013 respectively.
### The specific effects of the drug, including, for example, the pharmacological, psychoactive and toxicological effects.

Anabolic androgenic steroids relate to the male sex hormones (especially testosterone) and have effects that encourage male pattern sexual characteristics and increase tissue growth (especially muscle and bone).

Their use illicitly usually entails significantly higher doses than therapeutic doses (up to a factor of 1000 times) and higher doses may be associated with psychoactive effects (e.g. hypomania, increased aggression and dependency).

High doses have been associated in animal studies with death of nerve cells and damage to liver cells.

### The risk, if any, of the drug to public health and safety.

QH advises that the major public health issue relating to steroid use centres around increased cardiovascular disease, seen in the short term but more likely in the long term. The evidence of this arises from studies within industries known to use steroids: wrestling and weight lifters particularly die in their 50s and 60s as compared to the general population of around 70 to 80 years. Other health risks include: liver problems (mostly in animal studies involving benign or malignant growths in the liver); and nerve cells, including brain cells, may die as a response to high levels of steroids in the bloodstream.

Other risks are those seen with any injecting substance, particularly the spread of blood-borne viruses through sharing dirty needles.

The risks in terms of violent behaviour have not been studied in any prospective way, but is instead dependent on retrospective studies and case reports.

QH further advised that aggression and violence associated with illicit steroid use is likely to exist, but is best described as being unpredictable with no common factor found to determine a particular risk for the violent response to occur. That is, some individuals experience increased aggression when taking steroids in very large doses. The limited studies that exist do not identify a specific predictive factor as to which individuals will become aggressive.

The QPS advises that anecdotal reports have been received from regional police tasked with responding to alcohol fuelled violence in entertainment precincts stating that a portion of the individuals involved (victims and perpetrators) are physically larger and stronger than those in past years and display aggression akin to ‘roid rage’. It must be noted that these are merely observations and assumptions of the involved police officers. There has been no research or forensic analysis conducted to validate the reports or to ascertain if other drugs such as alcohol, amphetamine type stimulants or other psychoactive drugs are present and contributing to the reported behaviour.
### The therapeutic value, if any, of the drug.

QH advises that steroids have a therapeutic use in cases of male hypogonadism (underproduction of testosterone in the body of multiple causes), osteoporosis and some chronic muscle wasting conditions. Therapeutic doses do not have an associated psychoactive property reported.

Testosterone replacement may be given by a number of available pharmaceuticals (e.g. nandrolone, deco-durabolin, reandron, proviron) and may be given orally or by intramuscular injection.

### The potential for use of the drug to cause death.

No information available.

### The ability of the drug to create physical or psychological dependence.

High doses of these substances suppress the normal production of testosterone. Once the high doses cease the body may take weeks to months to produce normal levels again. This may result in a flat, low energy feeling that may encourage the user to restart steroids. As such this represent a risk for dependency.

### The classification and experience of the drug in other jurisdictions.

Steroids are controlled to some extent in all Australian jurisdictions either through criminal drug control legislation (like the DMA) or health regulations referencing the Commonwealth Standard for Uniform Scheduling of Medicines and poisons (SUSMP or Poisons Schedule). A summary is provided below.

The numbers and types of compounds that are regulated under the criminal drug legislation differ across State and Commonwealth jurisdictions.

Steroids are controlled as the Australian Border under prohibited imports regulations.

**New South Wales**

*Drugs Misuse and Trafficking Act 1985:* Offences of possession, supply, trafficking, manufacture offences for which penalties range from maximum two years imprisonment to life imprisonment.

*Poisons and Therapeutic Goods Act 1966:* offence of possession carrying maximum two years imprisonment.

**Victoria**

*Drugs, Poisons and Controlled Substances Act 1991:* Offences of possession, introduction of drug to another’s body, use, supply, trafficking for which penalties range from one year maximum to life imprisonment.

**South Australia**

*Controlled Substances Act 1984:* Offences of unlawful prescription, selling, supply, administration, manufacture, prescribing, possession for which penalties are maximum two years imprisonment.
The illicit drug market

Tasmania

*Misuse of Drugs Act 2001: Offences of manufacture, trafficking, supply, possess, use, administer to another, import for which penalties range from two years maximum to 21 years maximum.

*Poisons Act 1971: Offence of possession for which maximum penalty is two years imprisonment.

Australian Capital Territory

*Crimes Act 1900: Offences of unlawfully prescribing, supplying, possession and administration for which penalties range from maximum six months to five years imprisonment.

*Medicines, Poisons and Therapeutic Goods Act 2008: Offences of manufacture, obtain, possess, administer, issue purchase orders, prescribe for which penalties are maximum five years imprisonment.

Northern Territory

*Misuse of Drugs Act: Offences of supplying, manufacture, possession and administration for which penalties range from maximum two years to 25 years.

Western Australia

*Misuse of Drugs Act 1981: Offence of possession and use for which the maximum penalty is two years imprisonment.

*Poisons Act 1964: Offences of manufacture, distribution, supply, sale, administration for which fines apply.

*Medicines, Poisons and Therapeutic Goods Act 2008: Offences of obtaining, possession, administering, issuing purchase orders and prescribing for which the penalty is maximum five years.

Inconsistencies

MDPV, PMMA, and steroids provide examples of Schedule 1 drugs capable of being abused and which evidence suggests their prevalence in Queensland is indicative of increasing popularity in the illicit drug market. The effects of MDPV and PMMA on users are far more serious than the effects of steroids. Evidence suggests MDPV is highly potent at low level doses, in contrast to drugs such as heroin. The subjective effects of MDPV are likened to those of cocaine, amphetamine and MDMA which are drugs with a high degree of dependency and high doses can cause a raft of serious psychotic symptoms. MDPV has been linked to deaths.

In the submission relating to PMMA, the following was included, ‘It is upon the basis of the deaths from PMMA that it is recommended to be included in Schedule 1 rather than Schedule 2.’ Given that deaths occurred with both MDPV and PMMA and both drugs are highly dangerous, it is difficult to reconcile and understand why one drug was placed in Schedule 1 and one drug in Schedule 2. While it was not clearly stated in the recommendation, it is likely that the reason for this distinction was because PMMA was a derivative of a Schedule 1 drug, whilst MDPV is a derivative of a Schedule 2 drug. Whatever the rationale, the resulting effect is inconsistency between the schedules; where drugs with potential fatal consequences from use are subject to different maximum penalties.

The misuse of steroids is most often linked to bodybuilding and gain of increased muscle bulk. The long-term effects of abusing steroids include an increased risk of cardiovascular disease, liver problems, and nerve and...
brain cell damage. There is no evidence suggesting steroid abuse as a primary cause of death in an overdose type situation. There is no direct link to psychiatric symptoms after use, nor serious dependency issues. Despite this, steroids are classified as a Schedule 1 drug, inferentially more serious than MDPV.

Conclusion

It is the Commission’s view that the two-schedule regime raises a risk for inconsistency in scheduling. The scheduling of MDPV and PMMA provide an example. The link to deaths appears to be a primary reason why PMMA was classified as a Schedule 1 drug, yet the same process is not followed for MDPV. If the reason for the different classification of these two drugs was because of the classification of the drug of which they are a derivative, then this is another concern in the way in which drugs are placed in the schedule, particularly in the absence of an audit of existing drugs to ensure they are appropriately classified. The present system of classification sees some drugs being deemed as less serious than others, in circumstances where the effects of their use are as dangerous as the drugs in Schedule 1 and in many cases more dangerous than, for example, steroids—which are currently Schedule 1 drugs.

General and personal deterrence are important sentencing features in the Queensland criminal justice system. General deterrence is particularly relevant for offences which cause harm to individuals, the community and which are prevalent within society. Drug offending falls within this category. Further, the illicit drug market has and continues to be, a feature of the organised crime environment. The effectiveness of laws to deter criminal conduct rests on a number of features, one of which is the maximum penalties which apply to the prohibited conduct. Queensland’s dangerous drug laws carry strong maximum penalties; however, if those penalties are not readily discernable to the public, arguably that deterrent value is diminished. It is the Commission’s view that the multi-schedule approach used in Queensland injects a complexity into the penalty regime which renders it less transparent. In considering the issue of drug offending and maximum penalties in an organised crime context, the Commission notes the potential application of the Vicious Lawless Association Disestablishment Act 2013.

The Commission favours the approach taken in other Australian jurisdictions where all prescribed dangerous drugs are included in the one schedule and the type of drug does not dictate the applicable maximum penalty. The schedule should include a column containing threshold weights to determine jurisdiction and penalty.

If the view is taken that the current maximum penalties applicable for Schedule 1 drug offending should provide the benchmark, then a consequence of moving to a single-schedule regime is an increase in the applicable maximum penalties for producing, supplying and trafficking in current Schedule 2 drugs. The Commission is not concerned with such an increase, given the evidence as to the impacts of the illicit drug market on the economy and society and given the involvement of organised criminal activity.

The Commission would be concerned to see an increased maximum penalty applying to persons in possession of small quantities of Schedule 2 drugs; however, the move to a single-schedule regime will not impact on such persons. The offence of possessing a dangerous drug, whether Schedule 1 or Schedule 2 without a circumstances of aggravation has the same maximum penalty, being 15 years imprisonment. As such, this change in legislation would not impact upon low-level users of drugs and drug addicts who have possession for their own use.

The proposed amendment would have the following effect:

- Trafficking in a Schedule 2 dangerous drug, which currently has a maximum penalty of 20 years, will increase to 25 years.
- Supplying a Schedule 2 dangerous drug to a minor under 16 years currently has a maximum penalty of 25 years, and this would increase to life. Supply of a Schedule 2 drug with other circumstances of aggravation would increase from 20 years to 25 years imprisonment. Supplying without circumstances of aggravation would increase the maximum penalty from 15 years to 20 years.
- Producing a Schedule 2 dangerous drug in excess of the Schedule 3 quantity would increase from 20 years to 25 years. Producing a dangerous drug without the circumstance of aggravation would increase the maximum penalty from 15 years to 20 years.
• Possessing an amount of the drug under Schedule 3 quantity would not impact on the maximum penalty, though possession in excess of that schedule would increase the maximum from 20 years to up to 25 years.

The Commission is aware that some sectors of the community view cannabis as less dangerous than other illicit drugs. Cannabis is an illegal drug in most countries, although some jurisdictions—including some Australian jurisdictions—have decriminalised the possession of small quantities for personal use. Queensland has not followed such a course, and indeed the evidence before the Commission is that cannabis use is prevalent throughout Queensland, heavy use of cannabis is associated with a number of adverse health consequences, and organised crime groups are active within the cannabis market.

An amendment to the Drugs Misuse Act and Drugs Misuse Regulation to implement a one dangerous drug schedule regime with resulting increased maximum penalties will require consequential amendments to other provisions within the legislation concerning jurisdiction for disposition of the offences. Section 13 of the Drugs Misuse Act provides for the summary disposition of the offences of supply, produce and possess dangerous drugs in the circumstances where the maximum penalty does not exceed 15 years imprisonment. The Commission would recommend an amendment to section 13 to allow certain offences of supply and produce dangerous drugs to be dealt with summarily despite the penalty increase. The new drug Schedule could specify small quantities appropriately dealt with in the Magistrates Courts.

Recommendation

3.4 The Commission recommends that the Queensland Government amend the Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987 to omit the current distinction between types of dangerous drugs by including all dangerous drugs in the one Schedule. The maximum penalties that apply for offences relating to current Schedule 1 dangerous drugs should be retained and applied to all dangerous drugs. The quantities specified in Schedules 3 and 4 should be retained but moved to be included in the dangerous drug Schedule for ease of reference. Consequential amendments should be made to ensure appropriate offending can still be dealt with summarily.

3.4.2 Police powers in Queensland

The powers available to Queensland police officers to investigate offences and enforce the law are consolidated in the Police Powers and Responsibilities Act 2000 (Qld). Queensland police have wide-ranging powers to search persons, vehicles or premises when they have reasonable suspicion that drugs may be present. This section focuses on the search powers available to police officers in the context of drug offences.

A police officer may apply for a search warrant or, in certain circumstances, proceed in the absence of one. Section 150 of the Police Powers and Responsibilities Act provides the power for a police officer to apply for a warrant to, amongst other things, enter and search a place to obtain evidence of the commission of an offence. Generally such applications are made to a Justice of the Peace. In certain circumstances, the application must be to a Magistrate, and if entering and searching the place will cause structural damage to a building, the application is to a Supreme Court judge. Applications for search warrants must be sworn, and the section prescribes what must be contained in the application.

Warrants may only be issued in this manner when the issuer is satisfied there are reasonable grounds for suspecting the evidence averred to in the application is at the place or likely to be there within the next 72 hours. A police officer may rely on information provided through witnesses, investigative findings and intelligence to support the application.
Section 157 of the Police Powers and Responsibilities Act outlines the broad powers available to police officers when executing a search warrant. Relevant powers for search warrants relating to drug offences include:

- enter the place stated in the warrant and to stay on it for the time reasonably necessary to exercise powers authorised under the warrant and this section
- pass over, through, along or under another place to enter the relevant place
- search the relevant place for anything sought under the warrant
- open anything in the relevant place that is locked
- detain anyone at the relevant place for the time reasonably necessary to find out if the person has anything sought under the warrant
- detain a person on the relevant place for the time taken to search the place if police reasonably suspect the person has been involved in the commission of the relevant offence
- dig up land
- seize a thing found at the relevant place, or on a person found at the relevant place, that the police officer reasonably suspects may be warrant evidence or property to which the warrant relates
- photograph anything the police officer reasonably suspects may provide warrant evidence or property to which the warrant relates, whether or not the thing is seized under the warrant
- remove wall or ceiling linings or floors of a building, or panels of a vehicle, to search for warrant evidence or property.

In addition, a police officer may, if authorised under the warrant, do the following things:

- search anyone found at the relevant place for anything sought under the warrant that can be concealed on the person
- search anyone or anything in or on or about to board, or be put in or on, a transport vehicle
- take a vehicle to, and search for evidence of the commission of an offence that may be concealed in a vehicle at, a place with appropriate facilities for searching the vehicle.

It is evident that police have broad-ranging search powers under the Police Powers and Responsibilities Act to assist in the search and seizure of drugs and drug related evidence. However, police are not always going to be in a position to collate information and evidence in a sufficiently timely manner to allow an application for a search warrant to be made, at the risk of evidence being destroyed or removed. Accordingly, the Police Powers and Responsibilities Act allows the police to perform emergent searches.

Sections 29 and 30 of the Police Powers and Responsibilities Act deal with the searching of persons without a warrant. Section 29 provides the power to do so when a person is reasonably suspected of satisfying the prescribed circumstances outlined in section 30. The section further provides the power for a police officer to search a person if they reasonably suspect the person is a participant in a criminal organisation. The police officer is able to seize property in certain circumstances. The prescribed circumstances to satisfy section 29 include the belief that the person has something that may be:

- a weapon, knife or explosive the person may not lawfully possess, or another thing that the person is prohibited from possessing under a domestic violence order or an interstate domestic violence order
- an unlawful dangerous drug
- stolen property
- unlawfully obtained property
- tainted property
- something that may have been used, is being used, is intended to be used, or is primarily designed for use, as an implement of housebreaking, for unlawfully using or stealing a vehicle, or for the administration of a dangerous drug.
In addition to having the power to conduct an emergent search on a person, police also have the power to conduct an emergent search of a vehicle.

Section 31 of the Police Powers and Responsibilities Act is the relevant provision concerning the searching of a vehicle without a warrant. Section 31 empowers a police officer to stop a vehicle, detain it and its occupants, and search it for anything relevant to the circumstances for which it has been detained. In a similar way to section 30, section 32 outlines the prescribed circumstances for searching a vehicle in these circumstances. A police officer is empowered to take the vehicle to an appropriate facility to conduct a search, if it is impracticable to do so at the scene. The prescribed circumstances to satisfy section 31 include the belief that the vehicle is being used by, or is in the possession of a participant in a criminal organisation or that there is something in the vehicle that:

- may be a weapon or explosive a person may not lawfully possess, or another thing that the person is prohibited from possessing under a domestic violence order or an interstate domestic violence order
- may be an unlawful dangerous drug
- may be stolen property
- may be unlawfully obtained property
- may have been used, is being used, is intended to be used, or is primarily designed for use, as an implement of housebreaking, for unlawfully using or stealing a vehicle, or for the administration of a dangerous drug.

Section 160 of the Police Powers and Responsibilities Act allows a police officer to conduct a search if they reasonably suspect a thing at a place or in the possession of a person at a place is evidence of the commission of a Part 2 offence (Part 2 includes an indictable offence), and they suspect that the evidence may be concealed or destroyed unless the place is immediately entered and searched. The police officer is empowered by this section to enter and exercise search warrant powers, excluding the doing of any structural damage to a building.

The common threshold for the exercise of powers in each of these sections in the Police Powers and Responsibilities Act is a reasonable suspicion. In practical terms, this means the police officer must suspect on grounds that are reasonable in all the circumstances. Such a threshold enables police to search and seize drug-related items in circumstances where they are using their experience and knowledge without having time to obtain a pre-search warrant.

The QPS also has the ability to use telecommunication intercepts as a tool for the investigation of serious illicit drug matters. The Telecommunications Intercept Act (Qld) 2009 establishes a recording, reporting and inspection regime required under the Telecommunications (Interception and Access) Act (Cth) 1979 for the Commonwealth Minister to be able to declare the QPS to be an agency under the Commonwealth Act. Warrants are obtained under the Commonwealth Act or alternatively the Police Powers and Responsibilities Act, and must be in a prescribed form detailing, amongst other things, the length of the intended telecommunications intercept, the name of the person subject of the warrant, the facts and other background evidence relied upon to establish grounds for the intercept. Upon satisfying the Court of the grounds required to obtain a warrant, the QPS are able to gather invaluable evidence in a covert manner.

In addition to telecommunication intercepts, legislation also allows the QPS to use undercover officers during the investigation of controlled activity offences.

Controlled activity offence means—

(a) a seven year imprisonment offence; or
(b) an indictable offence mentioned in Schedule 2; or
(c) an indictable or simple offence mentioned in Schedule 5.

Officers are able to work undercover and interact with offenders involved in organised crime and the illicit drug trade in an attempt to extract further information and evidence. It is lawful for the officer to conceal their identity and the true purpose of their involvement. Further, acts committed by the officer that would
The illicit drug market

The Police Powers and Responsibilities Act also provides for the use of surveillance devices in criminal investigations. Such devices include data surveillance devices, listening devices, optical surveillance devices and tracking devices.

A police officer of at least the rank of inspector may apply to a Supreme Court judge (or a magistrate in the case of a tracking device only) for the issue of a surveillance device warrant if the officer reasonably believes that a relevant offence has been, is being, or is likely to be committed. A relevant offence is a seven-year imprisonment offence or an indictable offence mentioned in Schedule 2 of the Police Powers and Responsibilities Act.

When deciding an application the issuer must be mindful of the highly intrusive nature of a surveillance device warrant and have regard to certain issues such as the nature and gravity of the relevant offence, the extent to which the privacy of any person is likely to be affected, the existence of alternative ways of obtaining the evidence or information sought, the evidentiary or intelligence value of the information sought, and any submissions made by the Public Interest Monitor.

Detective Inspector Mark Slater of the QPS Drug Squad, in his interview with the Commission, was questioned as to whether he believed the current powers were sufficient for the Drug Squad in carrying out their duties. The Detective Inspector advised the Commission that, in his view, the powers were sufficient, and he had not been made aware of any difficulties his officers were having with these. He noted that many of the operations undertaken by the Drug Squad were tactical operations and, as such, they were not encountering any problems in obtaining a search warrant.

It is the Commission’s view that extensive search, seizure and covert investigative powers are available to Queensland police when investigating drug offending.

Commonwealth

The Australian Federal Police (AFP) operate under the Crimes Act 1914 and have wide-ranging powers to search persons, vehicles or premises when they suspect, on reasonable grounds, drugs may be present.

Section 3E of the Crimes Act provides that a Justice of the Peace or a Magistrate may issue a warrant to search a premises if satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises. The section goes on to provide that the issuer may issue a warrant authorising an ordinary search or a frisk search of a person if they are satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that the person has in his or her possession, or will within the next 72 hours have in his or her possession, any evidential material. The Justice or Magistrate when issuing a warrant must state a number of particulars as to the warrant when issuing it.

Once issued, an AFP officer when executing a warrant is authorised to do a number of things including:

- enter the warrant premises and, if the premises are a conveyance, enter the conveyance, wherever it is
- search for and record fingerprints found at the premises and take samples of things found at the premises for forensic purposes
- search the premises for the kinds of evidential material specified in the warrant, and seize things of that kind found at the premises
- seize other things found at the premises in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be evidential material in relation to the offence the subject of the warrant, another indictable offence or tainted property
The illicit drug market

• Seize things if the officer believes on reasonable grounds that seizure of the things is necessary to prevent their concealment, loss or destruction or their use in committing an offence.
• if the warrant so allows, conduct an ordinary search or a frisk search of a person at or near the premises if the executing officer or a constable assisting suspects on reasonable grounds that the person has any evidential material or seizable items in his or her possession.

If the warrant authorises the execution of a search on a person, then the police officer is authorised to search the person and to seize things found of the kind referred to in the warrant, record fingerprints from things located and take forensic samples from things located. They are further authorised to seize other things found in the course of the execution of the warrant which they believe on reasonable grounds to be evidential material in relation to an offence to which the warrant relates, or a thing relevant to another indictable offence, or tainted property if the police officer believes on reasonable grounds that seizure of the things is necessary to prevent their concealment, loss or destruction or their use in committing an offence.

Unlike the Police Powers and Responsibilities Act, the Crimes Act does not include a section dealing specifically with the search of persons or property without a warrant, with the exception of terrorism-related offences and searching of conveyances (vehicles, aircrafts or vessels). The section in the Crimes Act relating to searching of conveyances without a warrant is substantially similar to those in the Police Powers and Responsibilities Act allowing for searches without warrants.

Section 3T of the Crimes Act authorises a police officer who reasonably suspects that a thing relevant to an offence is in a conveyance and that it is necessary to execute a search in order to prevent the concealment, loss or destruction of it and that it is necessary to exercise this power in the absence of a warrant due to the circumstances being serious and urgent, to conduct a search. The police officer is empowered to stop and detain the conveyance, search it and seize the thing if located. If during the search the officer locates another thing relevant to an indictable offence, they are permitted to seize that if it is necessary to prevent its concealment, loss or destruction and it is necessary due to the circumstances being serious and urgent.

Summary

Both the Queensland and federal police have broad search and seizure powers conveyed upon them by State and Commonwealth legislation respectively. The relevant legislation allows police to effectively search for and seize drugs, appropriately detain and search drug-related offenders, and otherwise investigate illicit drug crime.

In its submission to the Commission, the QPS did not advocate for further powers.

3.4.3 Regulatory gaps

The Commission notes the absence of regulation around the sale and purchase of hydroponic equipment.

The evidence before the Commission is that cannabis use is prevalent throughout Queensland, that heavy use of cannabis is associated with a number of adverse health consequences, and that organised crime groups are active within the cannabis market.

In Queensland, the cannabis herb is generally sourced from plants grown locally, that is, both bush and hydroponic cannabis. Hydroponic cannabis that has been grown in a controlled environment tends to be of a more consistent and higher potency. According to the CCC, hydroponically grown cannabis is the dominant form available in the local market.

In Queensland, the sale and purchase of hydroponic equipment, used to cultivate indoor cannabis, is not subject to the same regulation that applies to the sale and purchase of laboratory equipment, used to unlawfully produce synthetic dangerous drugs and drug analogues.
The supply of laboratory glassware in Queensland is governed by Part 5A of the Drugs Misuse Act and Part 3 of the Drugs Misuse Regulation. That Part applies to the supply of a controlled substance or a controlled thing under a relevant transaction.58

Schedule 8B of the Drugs Misuse Regulation stipulates the following as controlled things:

- condenser
- distillation head
- heating mantle
- manual or mechanical pill press, including a pill press under repair, a modification of a pill press and parts for a pill press
- reaction vessel, including a reaction vessel under repair or a modification of a reaction vessel
- rotary evaporator
- splash head, including a splash head under repair or parts for a splash head.

Section 43D of the Drugs Misuse Act sets out the requirements for the supply of a controlled thing under a relevant transaction. These include a requirement for the seller to obtain from the recipient the documents specified under the Regulation, including proof of identity, the requirement to keep these documents for the required time under the Regulation and to maintain a transactions register.

Pursuant to section 43E of the Drugs Misuse Act, if a controlled thing is lost or stolen, there is an obligation to report the loss or theft to a police officer within two days of discovering the loss or theft.

The Drugs Misuse Regulation sets out the specific information to be produced and recorded in a supply of a controlled thing. Section 6(2) states that:

(2) The person must, before supplying the substance or thing, obtain from the recipient a document (an end user declaration) showing the following information –

(a) The recipient’s name and address, and if the recipient purports to obtain the substance of thing for another person, the other persons’ name and address;
(b) Details of the official document produced by the recipient under subsection (3) as evidence of the identity;
(c) The date and number of the written order for the supply of the substance or thing;
(d) The name and quantity of the substance or thing to be supplied;
(e) If a thing is supplied – the serial number or unique identifier of the thing;
(f) The date on which the substance of thing is to be supplied;
(g) The purpose for which the substance or thing is to be supplied.

(3) If the recipient is an individual, the person must, before supplying the substance or thing, require the recipient to produce an official document containing the recipient’s photograph (for example, a passport or driver licence) as evidence of the recipient’s identity.

(4) The person must, immediately the person supplied the substance or thing under the transaction, make an invoice for the supply of the substance or thing showing the following details –

(a) The recipient’s name and address;
(b) The recipient’s order number for the supply of the substance or thing;
(c) The date the substance was supplied;
(d) The name and quantity of the substance or thing supplied

Importantly, the person who supplied a controlled substance or thing must then give a copy of the end user declaration to the Commissioner of the QPS as soon as practicable.59 This is highly relevant because it provides the QPS with an opportunity to evaluate any purchases by persons and the reasons for those purchases. In the event a person is purchasing laboratory equipment in unusual or irregular circumstances, or if that person is purchasing equipment in large quantities or from a number of suppliers, then it would alert the QPS to some possible unlawful activity.

These provisions apply only to laboratory equipment in Queensland. In South Australia, an end user declaration scheme is used to regulate not only laboratory equipment but also hydroponic equipment. The relevant legislation is the Hydroponics Industry Control Act 2009 (SA) and the Hydroponics Industry Control
The illicit drug market

The Queensland Organised Crime Commission of Inquiry Regulations 2010 (SA). The purpose of the Act is to prevent criminal infiltration of the hydroponics industry, to prevent the misapplication of certain types of hydroponic equipment by monitoring its sale and supply, and for other purposes. Section 10 of the Act requires a person to hold a licence if they are carrying on the business of selling prescribed equipment by retail. The legislation goes on to provide for the things to be considered in granting a licence, suspension or revocations of licences, approval of hydroponic industry employees and various other requirements.

Part 3 of that Act deals with the sale of prescribed equipment. Prescribed equipment is defined in the Regulation to be:

- metal halide lights, high pressure sodium lights and mercury vapour lights of 400 watts or greater
- ballast boxes designed or intended for use in association with a light of a kind referred to above
- devices (including control gear, lamp mounts and reflectors) designed to amplify light or heat and capable of being used in association with a light of a kind referred to above carbon filters designed to filter air within a room, or from one area of a building to another or to outside
- units designed to contain plants and rotate around a light source so that the plants grow hydroponically while being exposed to a consistent degree of light or heat or both.

Section 23 of the Act provides that a licence holder must keep the information required by the Regulation in relation to each prescribed transaction occurring in the course of, or for the purposes of, the licence holder’s business. Section 12(1) of the Regulation outlines what information is required to be kept for the purposes of this section and includes:

- name, address and business name of the licence holder
- place where transaction occurred
- date and time of transaction
- description of prescribed equipment
- full name, address, date of birth of the purchaser of the equipment, and details of the identification produced to prove this identity and the name of the person to whom the identification was produced.

Section 12(2) of the Regulation provides that the licence holder must keep this information at the prescribed record-keeping location for a period of not less than seven years after the date on which the record is made. Those particulars must then be provided to the Commissioner of Police within 72 hours of the transaction occurring.

The South Australian Act places similar requirements upon those selling hydroponic equipment to those selling laboratory equipment that currently exist in Queensland.

Detective Inspector Slater of the QPS Drug Squad was asked about his views on whether he believed this type of regulation would be of use in Queensland. He advised that the end user declarations currently received in relation to the sale of laboratory equipment were currently monitored by the QPS Chemical Diversion Desk. While he accepted there would be resource implications to extending the scheme to hydroponic equipment, he believed such regulation would assist the police to monitor the movement of such equipment. In particular, Detective Inspector Slater noted that the sale of heat and lighting hydroponic equipment would be of interest to police because that is rarely used for any legitimate purpose and is something the police regularly see with hydroponic cannabis productions.

The Commission notes that extending the end user declaration scheme in Queensland to hydroponic equipment has the potential to prevent the misapplication of hydroponic equipment. However, such equipment is used by a large number of industries throughout Queensland for legitimate purposes and consultation would be required to identify the extent of any resource implications on such industries.

Potential benefits to the community in curbing cannabis production must be balanced against the impacts on industry.

On 25 November 2010, the former Queensland Parliament Social Development Committee tabled a report to Parliament on its inquiry into addressing cannabis-related harm in Queensland. As part of that report, the
The Committee recommended that the Queensland Government monitor developments in the hydroponics industry in Queensland and the effectiveness of the South Australian legislation regulating the hydroponics industry in that State.\textsuperscript{61}

The Government response was tabled on 25 February 2011. The Bligh Government supported the Committee’s recommendation. In responding, the then-Queensland Government advised that the standing inter-departmental working group on drug misuse legislation which is chaired by DJAG, would investigate the introduction of end user declarations for specified hydroponic products by the end of 2011. The working group would also continue to monitor the effectiveness of the South Australian legislation.\textsuperscript{62}

In responding to a Notice issued by the Commission, Mr David Mackie, Director-General of DJAG, advised as follows:

- The issue of end user declarations for specified hydroponic products was not investigated by the IDWG in 2011 following tabling of the Government response in February 2011 to the Parliamentary Committee’s report “Addressing Cannabis-related harm in Queensland”.
- The issue of end user declarations for hydroponic equipment was listed on the agenda for the IDWG meeting on 10 August 2012. However, the matter was not reached for discussion and it was not discussed.
- Strategic Policy has reviewed the records from subsequent meetings of the IDWG. It does not appear that the issue of end user declarations for hydroponic equipment has been revisited by the IDWG since 10 August 2012.

The Commission considers it unfortunate that the inter-departmental working group failed to implement the then-Government’s commitment to investigate the introduction of end user declarations for specified hydroponic equipment.

Regulating the sale and purchase of hydroponic equipment will increase the risk of detection for illicit cannabis producers and may deter persons from such illegal endeavours. The Commission notes the need for industry consultation in considering introducing such regulation and notes the potential for cross-border purchases of hydroponic equipment in those states and/or territories that do not have such regulation. This may be a matter for the government to raise at the National Law, Crime and Community Safety Council meeting.

\textbf{Recommendation}

\begin{quote}
3.5 The Commission recommends that the Queensland Government consider amending the \textit{Drugs Misuse Act 1986} and \textit{Drugs Misuse Regulation 1987} to extend the current end user declaration scheme to hydroponic equipment.
\end{quote}

With regards to any legislative inadequacies, the Commission considered the purchasing, supply and trafficking of dangerous drugs over the Internet. Such criminal activity is an emerging and concerning trend within Queensland with respect to the illicit drug market. The issue is considered in a separate part of the chapter.

\textbf{(Endnotes)}

1. Section 9 \textit{Drugs Misuse Act 1986 (Qld)}.
2. Section 6 \textit{Drugs Misuse Act 1986 (Qld)}.
3. Section 8 \textit{Drugs Misuse Act 1986 (Qld)}.
4. Section 5 \textit{Drugs Misuse Act 1986 (Qld)}.
5. Section 9(1)(a) \textit{Drugs Misuse Act 1986 (Qld)}.
6. Section 9(1)(b) \textit{Drugs Misuse Act 1986 (Qld)}.
7. Section 9(1)(c) \textit{Drugs Misuse Act 1986 (Qld)}.
8. Section 9(1)(d) \textit{Drugs Misuse Act 1986 (Qld)}.
9. Section 8(1)(a) \textit{Drugs Misuse Act 1986 (Qld)}.
10. Section 8(1)(b) \textit{Drugs Misuse Act 1986 (Qld)}.
11. Section 8(1)(c) \textit{Drugs Misuse Act 1986 (Qld)}.
12. Section 8(1)(d) \textit{Drugs Misuse Act 1986 (Qld)}.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Section 8(1)(e) Drugs Misuse Act 1986 (Qld).
Section 6(1)(a) Drugs Misuse Act 1986 (Qld).
Section 6(1)(b) Drugs Misuse Act 1986 (Qld).
Section 6(1)(c) Drugs Misuse Act 1986 (Qld).
Section 6(1)(d) – (f) Drugs Misuse Act 1986 (Qld).
Section 5(1)(a) Drugs Misuse Act 1986 (Qld).
Section 5(1)(b) Drugs Misuse Act 1986 (Qld).
Section 5(2) Drugs Misuse Act 1986 (Qld).
Section 5(3) Drugs Misuse Act 1986 (Qld).
Section 21, Drug Misuse and Trafficking Act 1995 (NSW)
Statutory Declaration of David Mackie, 1 June 2015, paras 3–5 [In-Confidence].
Statutory Declaration of David Mackie, 1 June 2015, para. 6 [In-Confidence].
Statutory Declaration of David Mackie, 1 June 2015, paras 14–15 [In-Confidence].
Transcript of Interview, Mark Slater, 1 July 2015, p. 14 [In-Confidence].
Transcript of Interview, Mark Slater, 1 July 2015, p. 15 [In-Confidence].
Notice to produce documents, David Mackie, 26 May 2015.
Explanatory Notes to Safe Night Out Legislation Amendment Bill 2014 (Qld).
Section 9(1)(c) Penalties and Sentences Act 1992 (Qld).
Section 150(5) Police Powers and Responsibilities Act 2000 (Qld).
Section 151 Police Powers and Responsibilities Act 2000 (Qld).
Section 29(1A) Police Powers and Responsibilities Act 2000 (Qld).
Section 29(2) Police Powers and Responsibilities Act 2000 (Qld).
Section 31(4) Police Powers and Responsibilities Act 2000 (Qld).
Section 160(3) Police Powers and Responsibilities Act 2000 (Qld).
Section 5(1) Telecommunications Interception Act (QLD) 2009.
Section 5(2) Telecommunications Interception Act (QLD) 2009.
Section 328-332 Police Powers and Responsibilities Act (QLD) 2000.
Section 45 Telecommunications (Interception and Access) Act (CTH) 1979.
Section 46 Telecommunications (Interception and Access) Act (CTH) 1979.
Section 221 Police Powers and Responsibilities Act (QLD) 2000.
Section 221 Police Powers and Responsibilities Act (QLD) 2000.
Chapter 13, Police Powers and Responsibilities Act (Qld) 1992
Transcript of Interview, Mark Slater, 1 July 2015, p. 24 [In-Confidence].
Section 3E(5) Crimes Act 1914 (Cth).
Section 3F(2)(b) Crimes Act 1914 (Cth).
Section 3F(2)(c) Crimes Act 1914 (Cth).
Section 3T(1) Crimes Act 1914 (Cth).
Section 3T(2) Crimes Act 1914 (Cth).
Section 3T(3) Crimes Act 1914 (Cth).
Section 43B, Drugs Misuse Act 1986 (Qld)
Section 5(1) Drugs Misuse Act 1986 (Qld).
3.5 Related activities

The Commission’s Terms of Reference required the Commission to inquire into the extent that entities involved in organised crime use, or provide the services of, activities that enable or facilitate organised crime in Queensland, with particular emphasis on the following:

- money laundering
- cyber and technology-enabled crime
- identity crime
- violence and extortion
- professional facilitators, including but not limited to accountants, lawyers, financial advisers, real estate agents, IT experts, technical security experts and chemists.

These ‘facilitating’ activities are often referred to by law enforcement and intelligence agencies as ‘enabling activities’. Enabling activities are activities that play a role in facilitating or enabling organised crime, but are not an end activity in themselves. Money laundering is an example of this. The act of laundering money would not be necessary if there were no illegal funds to launder in the first place, such funds having been acquired through illicit activities.

Persons with special skills or access to special information may support organised crime, knowingly or unknowingly. These are known as ‘professional facilitators’. Facilitators with specific skill sets (such as information technology specialists, accountants, lawyers and bankers) play a vital role, sometimes unintentionally, in assisting criminal networks operate undetected and seamlessly across both legitimate and illicit markets.

With regards to the illicit drug market in Queensland, the key enabling activities focused on by the Commission are Internet-enabled crime, violence and extortion, and any role played by pharmacists and solicitors.

(Endnotes)


3.5.1 The Internet

According to the United Nations International Telecommunications Union, 3.2 billion people are using the Internet in 2015. With the current world population at 7.2 billion, this means that one in 2.25 people are connected. Business and banking is conducted online, and with the massive uptake of social networking, people are increasingly sharing personal information online.
The Internet is an integral part of Australians’ everyday lives. The Australian Bureau of Statistics advises that in 2012–2013, over 80 per cent of Australian households had Internet access, representing 7.3 million households. Almost every household with children under 15 years of age had access to the Internet at home (96%). Of those households with Internet access, four out of five households accessed the Internet every day. Seventy-six per cent of Internet users purchased goods or services online.

Unfortunately, the global uptake of the Internet has created opportunities for criminal exploitation, in particular with regards to dealing in contraband.

The Surface Web

Most people associate the Internet with the term World Wide Web. This is a part of the Internet which is readily accessible through a web browser. Directories and search engines such as Google and Yahoo enable people to access registered web sites and to converse through messenger sites and face-to-face programs. This part of the Internet is often referred to as the ‘Surface Web’.

The Surface Web is characterised by the ability to monitor communications and interactions between users. This is achieved through a store-and-forward model that is analogous to sending a letter in the mail. Whenever someone accesses part of the Surface Web, they are directed to an IP address for their ultimate destination. The user, in turn, also has an IP address. This is similar to someone sending a letter with the addressee on the front of the envelope and the return address on the rear. At any time, someone is able to determine where the mail is going to, and where it has come from. Similarly, with the Surface Web, an IP address reveals the originating computer and where it has been.

The Darknet

The ‘Darknet’ refers to the Internet that is not part of the World Wide Web. It is characterised by encrypted pathways and anonymity for users and services.

The Darknet allows hidden areas of the Internet to be accessed through special connections or routers, remaining decentralised and designed to function without a central authority. The browsers most often used to access the Darknet are Tor, Freenet and I2P. This chapter focuses on Tor.

Tor

Tor, otherwise known as ‘the onion router’, was developed in 2002 by the United States Naval Research Laboratory. Its purpose was to protect government communications by allowing the Surface Web to be accessed without an IP address leaving a digital footprint. The technology was upgraded to allow access to, and sharing of, information within the Tor network. This is one part of the Darknet where it can only be accessed if you have the Tor program on your computer.

Although Tor is still used by the United States Navy, its ongoing development is overseen by Tor Project Incorporated—a non-profit organisation funded by multiple parties, including the United States Federal Government.

Tor works by routing data through a randomly selected path of relay computers. A computer becomes a relay when the user installs Tor and selects the option to relay data through that computer. The data is encrypted in multiple layers of encryption. Each relay computer ‘peels’ away a layer of encryption (like a layer of onion – hence the name Tor – the onion router) before sending the data to the next relay.

If the data is destined for the Surface Web, the final relay is the ‘exit node’, an option that allows a relay to send data into the Surface Web. The exit node peels away the final layer of encryption before passing the data onto the destination. The destination, however, can only trace the data back to the exit node (or if the destination is a hidden service within the Tor network, to the last relay). This effectively conceals the IP address of the originating computer, thus rendering attempts to trace the location of the computer ineffective.
The illicit drug market

It is this level of anonymity that makes Tor attractive to those who wish to conduct their online activities without their movements being traced. Tor is used for legitimate purposes as well as illegal purposes. In some cases, dissidents in nations with authoritarian regimes are able to communicate with the surface web using the program.\textsuperscript{10} The ability to transmit and retrieve information anonymously is also attractive to those in the business world who wish to prevent competitors from accessing highly sought-after information and material. However, it is easy to see why this kind of environment would also attract those wishing to conduct illegal activities. Some of the illicit services and activities available on Tor include:

- drug dealing
- weapons dealing
- money laundering
- illegal gambling
- sex tourism
- paedophilia networks
- child exploitation material
- contract killing.\textsuperscript{11}

The Internet and drugs

For many years, the Surface Web has facilitated the commission of drug-related offences. Originally, the issue was pharmaceuticals. In 2009, the United Nations delivered a report entitled *Guidelines for Governments on Preventing the Illegal Sale of Internationally Controlled Substances through the Internet*.\textsuperscript{12} It detailed how the illegal sale of pharmaceuticals was facilitated by websites that purported to be Internet pharmacies, whereas in reality, they were organised crime groups participating in the acquisition and supply of pharmaceutical drugs.\textsuperscript{13} The report recommended the implementation of 25 guidelines to prevent the spread of illegal online pharmacies taking advantage of the opportunities made available by the Internet.

With the emergence of social media and new ways to interact online, the Internet increasingly became a highway of communication between those wanting to sell and those wanting to acquire drugs. The Commission is aware that within Queensland, there have been instances of offenders using networked computer games to arrange drug-related offences. When the game is connected to the Internet, other players are able to converse during gameplay. This has allowed some organised crime groups to discuss drug-related offences without the risk of traditional telephone intercept methods being used. The borderless world made available by the Internet allows individuals to access the drug market without being limited by traditional methods of contact.

Besides allowing for the ability to purchase and supply dangerous drugs, the Internet also allows organised crime groups to recruit members and communicate about their targets and related offences. The Commission is aware of instances of offenders using Facebook to communicate about drug sales, as well as to recruit individuals to commit property-related offences to fund the drug enterprise. These platforms give organised crime groups access to individuals who can be filtered according to their interests, locations and contacts.\textsuperscript{14}

Silk Road and life after

In February 2011, online drug-related offences entered the Darknet in a manner not seen before. With the creation of Silk Road, the Darknet turned into a shopping centre for illicit drugs, reminiscent of eBay. Silk Road was a marketplace for the purchase and sale of illicit drugs. It acted as an open market available to anyone with access to the Darknet through Tor or similar programs.\textsuperscript{15} With the click of a button, those looking to source drugs could read through a list of desired drugs, and the ‘history’ of the seller. Comments were left regarding the quality of products previously sold, as well as the purity of certain drugs. Additionally, those willing to sell drugs were met with the same anonymity amidst the shadows of the Darknet. The key to Silk Road’s success was its anonymity and quality control.\textsuperscript{16}
Substances sold on Silk Road were available to be purchased and sold within Australia or around the world. Drugs were placed into nine categories: cannabis, dissociatives, ecstasy, opioids, precursors, prescription, psychedelics, stimulants and other. These groups were then broken into subgroups. Within the subgroups, a list of sellers were made available to the buyer. Each seller had a rating that indicated buyer satisfaction, as well as comments and information about where the drug would be shipped from. Most of the drugs also referenced figures as to their purity. The majority of drugs shipping from overseas were far cheaper than the equivalent drug and amount in Australia, as indicated below.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cocaine</td>
<td>1 gram</td>
<td>$116.00</td>
<td>$363.00</td>
<td>$300.00</td>
</tr>
<tr>
<td>MDMA</td>
<td>1 gram</td>
<td>$45.00</td>
<td>$225.00</td>
<td>$200.00</td>
</tr>
<tr>
<td>MDMA (Pill)</td>
<td>1 pill</td>
<td>$10.00</td>
<td>$31.00</td>
<td>$25.00</td>
</tr>
<tr>
<td>Methylamphetamine powder</td>
<td>1 gram</td>
<td>$19.00</td>
<td>$147.00</td>
<td>$300.00</td>
</tr>
<tr>
<td>Methylamphetamine Crystal (‘ice’)</td>
<td>1 gram</td>
<td>$125.00</td>
<td>$574.00</td>
<td>$700.00</td>
</tr>
</tbody>
</table>

An FBI operation successfully shut down Silk Road in October 2013. However, since its closure, multiple new websites have emerged to take its place. In November 2014, a joint international law enforcement operation called Operation Onymous resulted in the closure of Silk Road 2.0 and many other sites. Between July and December 2014, a total of 23 Darknet drug marketplaces were identified, with 12 closing during the same period. This is the greatest proliferation of new marketplaces since August 2013, as well as the largest number of site closures.

However, according to the Crime and Corruption Commission (CCC), the closing of marketplaces on the Darknet—in particular Silk Road—has had little impact on those wanting to take advantage of the anonymity afforded when trading in drugs through this service.

The most commonly available drugs on the marketplaces are cannabis, MDMA/‘ecstasy’ and pharmaceuticals.

**Internet and the mail post**

The international mailing system is being used to distribute drugs purchased online, negating the need for face-to-face meetings, and providing a further level of anonymity to buyers and sellers. As opposed to traditional drug trafficking, which may involve large volumes of drugs being moved at any one time, trafficking via mail allows low volume, high-frequency importations.

In an attempt to further avoid detection, sellers have also sold decoy packages that contain only drug scent, to identify potential interest from law enforcement agencies. Packaging is also changing regularly. Buyers are also employing their own tactics to avoid detection, including opening multiple post office boxes in fake names. In one case, the offender opened ten post office boxes at different locations using false driver’s licenses as identification. In addition to these, he also opened additional mail boxes with a private mail...
The illicit drug market

Queensland Organised Crime Commission of Inquiry

franchising agency, again using false identification. This allowed his supplier in Thailand to send the cocaine being imported to various addresses in an attempt to avoid detection from the authorities.28

The ability to traffic in drugs through Australia Post allows organised crime groups to reach a larger geographical base than if they were employing traditional ‘on-the-ground’ techniques.

Virtual currency

To facilitate the purchase of drugs online while avoiding detection, transactions are conducted using virtual currency. Virtual currencies exist only in digital form, and originated from online multiplayer computer games, where they are still used legally. However, some investigations have suggested that online gaming has been used to launder money through virtual currencies.29 Despite originating from legal beginnings, virtual currencies now play an important role in illegal online activity. They are unregulated and have no central authority guaranteeing their value. They can be purchased through ordinary forms of payment (cash, cheque or credit card) and provide the following features:

- facilitate anonymity: no identifying details or accounts are required to purchase or sell virtual currencies
- are encrypted: using cryptography to authenticate transactions and anonymous accounts through digital signing and cryptographic proof-of-work
- make transactions difficult to trace: due to the lack of accounts, companies, banks, regulation and geographic borders
- are ideal for any illicit activities with a financial component.30

Although there are a number of operating virtual currencies, the most commonly referred-to currency with respect to drugs and the Internet is Bitcoin.31

Bitcoins are produced by solving complex cryptographic algorithms with a computer. The Bitcoin system is designed to make Bitcoins increasingly difficult to produce over time, requiring increasing computational power. The amount of Bitcoins automatically awarded for each solved algorithm will also decrease, until an overall limit of 21 million Bitcoins is reached.32

Due to the limited nature of Bitcoin’s production, its value is more akin to a share than currency, fluctuating frequently, and often greatly. As demand increases, so does the price. In 2011, one Bitcoin rose from $0.30USD to $32USD before returning to $2USD.33 During the 2012–2013 Cypriot Financial Crisis, Bitcoin rose to $266USD on 10 April 2013, before crashing to around $50USD.34 Today, one Bitcoin is worth approximately $358AUD.35

The unregulated environment of Bitcoin and the anonymity of transactions make Bitcoin attractive to organised crime groups. Queensland-based offenders have been identified using Bitcoins to purchase drugs through the Darknet. Because of the legal use of Bitcoin, there are currently no laws in Australia against the currency. Bitcoin users also avoid cash transaction recording processes (e.g., through AUSTRAC).36

The first Bitcoin ATM to be introduced in Queensland was installed in May 2014. At the time, it was one of only two Bitcoin ATMs in existence in Australia. During the closure of a CCC operation, the Bitcoin ATM was seized to retrieve digital evidence from the ATM storage media.37 After finding no evidence of being linked to any criminal activity, the Bitcoin ATM was returned to its owner in April 2015.38
Illicit drug marketplaces on the Darknet operate through an escrow system. Escrow refers generally to where money is held by a third party until the transaction is complete. Half of the current marketplaces operate on a multi-signature escrow, with the other half operating on a centralised system. In a centralised system, funds are held until the buyer acknowledges receipt of the product. Multi-signature systems require two unique key strokes to be entered before the payment is released. This key stroke can be entered by the buyer, seller or third party. 39

Law enforcement

The then-Crime and Misconduct Commission released a report in 2013 with the following key findings:

- Highly secure communication technologies are increasingly employed by organised crime groups across Queensland. Law enforcement investigations are being impeded, regardless of whether a group deliberately seeks out secure technologies or incidentally benefits from the high default security measures on commonly used devices and applications.
- New technologies are facilitating multi-jurisdictional offending, as Queensland organised crime groups network more easily with groups based interstate and overseas.
- Although the use of telecommunication intercepts by law enforcement is acknowledged as being a very useful investigative tool, the emergence of new telecommunication devices and complex encryption software is likely to impact on the capability of agencies to target higher level serious and organised crime and technology-savvy new entrants into criminal markets. 40

The Queensland Police Service (QPS) expects that organised crime groups involved in the illicit drug market will start to migrate to the cyber environment due to the perception of a low risk of identification with high rewards offered by parts of the Internet, including the Darknet. 42 This theory has, in part, been supported by an increase in the importation of illicit drugs via secure online Darknet marketplaces, which may be increasing the availability of drugs in Queensland. The ease at which one can become connected to the Internet also means a broader range of people can move in and out of the market at will. 42

A main issue for law enforcement is the inability to accurately trace communications made online to particular individuals. Network configurations used by some telecommunication companies are such that law enforcement authorities are unable to locate the particular individuals using the service. Organised criminals have a vested interest in operating below the radar and in such a way that any prosecution of charges would bring about difficulties in identifying parties involved in the offences.
The CCC identifies the rate of development of organised crime groups; developments that mirror large corporations. There is a centralisation of operations, greater connectivity through the Internet and other forms of telecommunication, growing sophistication, increased professionalism and long-term strategic planning geared towards growth.43

The CCC also identifies that the increase in popularity of the Darknet method of purchasing and selling drugs, can, in part, be attributed to the lowered risk of face-to-face violence and physical threat.44 Drugs can be exchanged without meeting in public, which hampers traditional policing techniques. Without the need to run a drug trafficking syndicate, overall ‘on the ground’ costs are reduced for the organised crime group.45 Without the need for drugs to pass through multiple hands, it is expected that the purity of drugs will increase while costs remain low. While the Darknet is of great concern to law enforcement authorities, the sale of drugs online through social media platforms and chat rooms is increasing in popularity. These activities occurring on the surface web are much easier for law enforcement authorities to monitor and intervene in, and the QPS should continue to target these areas.

It is the Commission’s view that those involved in the illicit drug market, including organised crime groups, will increasingly use the Darknet.

It would be impossible for any single agency to effectively combat organised crime and drugs on the Internet. Collaboration needs to occur between agencies within Queensland as well as within Australia and around the world. Operation Onymous provides a good example of a successful initiative involving multiple agencies from across the world, working together to locate and close Darknet drug marketplaces.

As identified by the then Crime and Misconduct Commission in its 2013 report,46 there are growing issues with the use of telecommunication intercepts to gather evidence in drug investigations, due to the adaptation and modifications occurring within encrypted forms of communication. Evidence suggests it is only when drugs have been intercepted in the delivery process that arrests have been made. This is, in part, due to the anonymity provided by the Darknet, such that the online process is undetectable. However, this results in little being known about the groups behind the sales. Traditional telecommunication intercept methods are no match for the Darknet.

The then-Crime and Misconduct Commission reported in 2012 that formulating an effective and efficient law enforcement response that can operate across jurisdictions and is sufficiently expert in this highly technical area of the Darknet is challenging. While the law enforcement expertise is growing, law enforcement resource allocations to this area are unlikely to match the investment of the world-wide networks of volunteers in the continual development of that technology.47

In responding to a Notice issued by the Commission, Deputy Commissioner Ross Barnett of the QPS advised of the QPS approach:

- The QPS does not have dedicated officers tasked with monitoring internet activity relating to the purchase or supply of drugs. The QPS acknowledges that the sourcing of drugs using the internet is an emerging issue. However, focus has been placed on more traditional means of drug distribution as internet activity is reliant upon mail and parcel deliveries. Generally, smaller quantities of drugs are delivered by parcel or general mail often to end users or small scale suppliers, compared to quantities trafficked by other methods.

- Task Force Jericho, which comprises QPS, Australian Federal Police and Border Force officers do provide a response with respect to drugs destined for Queensland …

- The QPS responds to internet activity in relation to the purchase and supply of drugs when such matters are identified through intelligence, received via Crimestoppers, or received through liaison with other law enforcement agencies.48
The Commission has identified the purchase, supply and trafficking of drugs over the Internet as an emerging trend within the drug industry in Queensland. In its submission to the Commission, the QPS stated that it expects organised crime groups involved in the illicit drug market to migrate to the cyber environment. However, the QPS is not actively monitoring the Internet or Darknet for the activities of those involved in this emerging area. The Commission understands that two QPS officers are assigned to Taskforce Jericho, but their work is focused on a particular mail exchange and the parcels coming into that exchange destined for Queensland. While this work is clearly necessary, it is the Commission’s view that the QPS could take a more active role in the monitoring of the Internet for activity, with the aim of stemming the flow of these drugs into the state.

Similar to Taskforce Argos with online child sex offending, the QPS could conduct covert monitoring of online activities to identify drug activity occurring within the state. While most of the online activity occurs over the Darknet—with its concomitant problems of encryption and anonymity associated with that activity—there are a number of ways in which those specialised in online offending could attempt to infiltrate practices pertaining to the purchasing or supplying of drugs to persons in Queensland. Despite technologically savvy individuals or groups unlikely to make errors when using the Darknet, less-skilled or cautious people will make mistakes or misuse the features. It is at this point that police need to be trained to pick up on these errors and begin to gather evidence to allow successful arrest and prosecution. Together with traditional policing methods such as surveillance of post office boxes where these parcels are to be delivered, it would be likely to have an impact on this area of the drug industry in Queensland. At the very least, the Commission is of the view that the QPS needs to address this issue by allocating specialised officers to this emerging area.

While it is accepted that this is a new and emerging area with detection and investigation difficulties, it is an area that warrants focus by law enforcement. The QPS has noted that the volume of drugs coming in through the mail from Internet-related activity is believed to be low, and often destined for small-scale suppliers and end users. However, there is a concern that organised crime groups will exploit and expand into this market.

The Commission is particularly concerned about the Internet illicit drug market, because it attracts persons who may not otherwise be involved in the purchasing of drugs through traditional methods. An individual who has never come into contact with criminal elements may be highly reluctant to have direct physical dealings with a drug supplier, but may feel safe and protected in purchasing such contraband online. This circumstance has the potential to significantly increase the uptake of individuals using dangerous drugs, and increase the uptake of individuals sourcing drugs on the Internet to then on-sell.

With regards to the approach of law enforcement, the Commission supports the partnership approach evidenced in Taskforce Jericho. Inter-jurisdiction co-operation is vital. The Internet—particularly the Darknet—is ever-evolving. Law enforcement agencies must continue to learn, adapt and change policing methodologies to counter the marketplaces. The biggest challenge for agencies is to evolve in a way similar to the Internet—continually.

**Legislative inadequacy**

The Internet—particularly the Darknet—creates a low-risk environment for individuals and organised crime groups to purchase and sell dangerous drugs. The anonymity offered by encryption-based services and supplying via the post provides protection for offenders.

General and personal deterrence are important sentencing features in the Queensland’s criminal justice system. General deterrence is particularly important for offences that cause harm to individuals and the community, and which are prevalent within society. The fear of severe punishment does, and will, prevent the commission of many offences that would have been committed if it was thought that the offender would escape without punishment, or only with light punishment.
The offences provided in Queensland’s *Drugs Misuse Act 1986* of supplying and trafficking in dangerous drugs apply where the Internet is used to conduct such illicit business and such offences carry strong maximum penalties. However, Queensland’s dangerous drugs laws do not treat such dealings using the Internet as a circumstance of aggravation attracting higher maximum penalties.

Where illegal drugs are unlawfully imported or exported into and out of Australia, including using the Internet, the offences in Division 307 of Chapter 9 of the *Criminal Code Act 1995* (Cth) apply. The following offences apply and carry strong maximum penalties:

- importing and exporting border controlled drugs or plants (sections 307.1 – 307.4)
- possessing unlawfully imported border controlled drugs or plants (sections 307.5 – 307.7)
- possessing border controlled drugs or plants reasonably suspected of being unlawfully imported (sections 307.8 – 307.10)
- importing and exporting border controlled precursors (sections 307.11 – 307.13)

The Commonwealth Director of Public Prosecutions has identified 68 matters involving border controlled drugs, controlled drugs or Tier 1 goods where proceedings were commenced between 1 January 2013 and 19 June 2015 in Queensland. Of those matters identified, eight were reported to involve the use of the Internet to purchase or supply relevant drugs. These matters resulted in charges including conspiracy to traffic in a commercial quantity of a border controlled drug, importing a marketable quantity of a border controlled drug, possessing a dangerous drug and importing Tier 1 goods.\(^53\)

In the United States, illicit drugs are regulated by Title 21 of the *United States Code: The Controlled Substances Act*. This Act contains specific offences dealing with the sale of drugs over the Internet. Section 841(g) prescribes an offence of Internet sale of date rape drugs and section 841(h) outlines offences involving the dispensing of controlled substances by means of the Internet.

An examination of all Australian states and territories, including the Commonwealth, reveals that no such specific provisions exist. Given that such activity has been identified as an emerging trend, and given the social and economic impacts of drug crime on the Queensland community, the Commission is of the view that dealing in drugs over the Internet should be specifically prohibited, and subject to higher maximum penalties, in order to deter and curb this growing illicit market.

The Commission recommends amending the offences in the Drugs Misuse Act of possessing, supplying and trafficking in, dangerous drugs to create a new circumstance of aggravation. With regards to the offences of supplying and trafficking, the circumstance of aggravation will apply where the Internet is used to facilitate the offence. The circumstance of aggravation will apply to the offence of possessing a dangerous drug where the Internet is used to procure the drug.

The circumstance of aggravation will attract an additional five years to the maximum penalty otherwise applicable. For the offence of supplying a dangerous drug, the intention is to amend section 6(2) to include a further aggravated supply. For offences that carry a maximum penalty of 25 years imprisonment, the intention is that the circumstance of aggravation will raise the penalty to life imprisonment in accordance with the penalty regime currently in place.

Therefore, by way of example, if the person was charged with supplying a Schedule 1 dangerous drug and there was a circumstance of aggravation that the conduct occurred over the Internet, then that person would be liable to a maximum penalty of 25 years imprisonment rather than the current 20 year maximum penalty which applies to the simpliciter offence.
The Commission notes that the Criminal Code uses the term ‘electronic communication’ in a number of offences. The term ‘electronic communication’ is defined to mean email, Internet chat rooms, SMS messages, real time audio/video or other similar communication. However, it is the Commission’s intention that the proposed circumstance of aggravation will apply only to conduct occurring over the Internet (Surface Web or Darknet), including through chat rooms and gaming consoles that utilise the Internet. It is not intended to capture emails, SMS messages and telephone conversations.

Recommendations

The Commission recommends that:

3.6 The Queensland Police Service invest further resources into the area of online drug offending. In particular, additional police officers with sufficient training and expertise in cybercrime, be tasked to monitor online activity, with a view to infiltrating the activities of those purchasing and selling drugs over the Internet.

3.7 The Queensland Government amend the Drugs Misuse Act 1986 to apply aggravated penalties to the offences of possessing, supplying and trafficking in dangerous drugs where such conduct is facilitated by the Internet. The circumstance of aggravation would attract an additional five years. This will increase the maximum penalties to 20 years, 25 years, and life imprisonment.

(Endnotes)


5 Available at www.freenetproject.org (accessed 13 August 2015).

6 Available at www.i2p2.de (accessed 13 August 2015).


13 International Narcotics Control Board. (2009). Guidelines for Governments on


27. Consultations – Meeting Notes – Organised Crime Markets Assessment 2012 – Illicit drugs, Australian Customs and Border Protection Service, p. 3 [In-Confidence].


3.5.2 Pharmacists

The Commission’s Terms of Reference required the Commission to examine the role that chemists may play in enabling or facilitating organised crime in Queensland.

The term ‘chemist’ refers to a person authorised to dispense medicinal drugs, but it can also mean a person engaged in chemical research or experiments.\(^1\) For the purposes of the Inquiry, the Commission has interpreted the reference to chemists as a reference to people authorised to dispense medicinal drugs. Queensland legislation such as the Pharmacy Business Ownership Act 2001 refers to a person registered under the Health Practitioner Regulation National Law to practise in the profession of pharmacy as a ‘pharmacist’, and that term is used in this chapter.

The most obvious way in which pharmacists might enable the activities of organised crime is through the dispensing of precursor drugs that are used by criminals to produce illicit drugs.
A pharmacist has a duty to make the care of the customer their first concern, and to practice safely and effectively. The primary role of a pharmacist is to provide customers with information relating to prescription medication and other substances, as well as the dispensing of these items. Dispensing of medicines that have the potential to cause harm if misused or abused is the area of most concern when examining links between pharmacists and the illicit drug market. Despite a pharmacist’s best intention to comply with guidelines and legislation, they may be targeted by criminals—including organised crime groups—wishing to obtain precursor drugs to be made into illicit drugs.

For example, methylamphetamine is produced primarily from the precursor drug pseudoephedrine. The precursor’s molecular structure can be modified through a series of chemical reactions to produce methylamphetamine. Pseudoephedrine is classified as a Schedule 3 drug in the Poisons Standard and is a Schedule 6 controlled substance in Queensland’s Drugs Misuse Regulation 1987. This means that pseudoephedrine is a pharmacist-only medicine, which may be obtained without prescription, but must be sold as an ‘over the counter’ product. Because of this classification, pharmacists are required to ensure that these products are only provided in appropriate circumstances.

Queensland has the highest number of detected clandestine drug laboratories in Australia, accounting for 45.8 per cent of the country’s total number of detected labs. Of those detected, 270 were identified as being used for the production of amphetamine-type stimulants. This number is the highest in Australia, accounting for 44.4 per cent of amphetamine-type-stimulant labs detected in the country. It is clear that there is a significant market for methylamphetamine in Queensland and, as discussed earlier in the report, organised crime has a high level of involvement in the methylamphetamine market.

Pseudoephedrine remains the most commonly used ingredient in the making of methylamphetamine. Investigations suggest that pharmacists—specifically those who have poor prescribing practices and prescribe (knowingly or otherwise) larger-than-required quantities of pseudoephedrine—are the main source of the ingredient.

Regulation

Pharmacists are subject to a number of guidelines and pieces of legislation. The Queensland Acts relevant to pharmacists include the Pharmacy Business Ownership Act, the Health Practitioner Regulation National Law Act 2009 and the Health (Drugs and Poisons) Regulation 1996. In addition, pharmacists practicing in Queensland are subject to the Code of Conduct, Guidelines on Practice, and Guidelines for Dispensing of Medicines, as issued by the Pharmacy Board of Australia.

A pharmacist must be registered with the Pharmacy Board of Australia (the Board) in order to practice pharmacy. The Board must be satisfied that the pharmacist is suitable to hold general registration. Factors to be taken into consideration when registering a pharmacist include whether or not they have a criminal history, and any history of unprofessional conduct. Registration is renewed annually, with a pharmacist required to provide a statement outlining any changes to their criminal history or details of any unprofessional conduct. Pharmacists are also required to inform the Board of any relevant event that occurs between registration renewals. A relevant event can include instances such as being charged with an offence punishable by 12 months imprisonment or more, or being convicted of an offence punishable by any term of imprisonment.

In addition to having an obligation to adhere to certain regulations as individuals, pharmacists also have an obligation to report other pharmacists if those other pharmacists engage in notifiable conduct. If a pharmacist is seen to place the public at risk of harm by operating in a manner that departs from accepted professional standards, the National Board must be notified. The Board may take immediate action and suspend the registration of a pharmacist due to their conduct or performance. The matter may then either be determined by the performance and professional standards panel, or, in more serious cases, be referred to the Queensland Civil and Administrative Tribunal (QCAT) for final determination.
If QCAT makes a decision that the practitioner has engaged in unsatisfactory professional conduct, unprofessional conduct, or professional misconduct, or that the practitioner has an impairment or that the practitioner’s registration was improperly obtained, then certain consequences may occur. QCAT has the power to reprimand a pharmacist, place conditions on a registration, or suspend or cancel a pharmacist’s registration. Under previous legislative requirements, the relevant tribunal was required to stipulate a time frame within which the practitioner must not be registered, however, there is no longer any requirement under the current Act to stipulate a time frame. By implication, the Pharmacy Board determines the length of de-registration.

A pharmacist must not dispense pseudoephedrine without adopting a ‘quality standard’. A quality standard for dispensing pseudoephedrine is a document that states the standard for carrying out the activity of dispensing, as well as how the standard is met. Pharmacists are also required to obtain an endorsement to dispense pseudoephedrine from the Pharmacy Board of Australia. This process involves a written application where the suitability of the pharmacist is considered. In deciding suitability, the Board may have regard to things such as the person’s knowledge and understanding of their obligations, the person’s qualifications and experience, the person’s character and standing, or any previous convictions the person has had under the Regulation.

There must be a log containing an accurate stock-take of the controlled drug, which may be audited at any time by the Board. This log is required to be kept for a period of two years, and it must be accessible online by both the Director-General of Queensland Health and by the Commissioner of Police.

A pharmacist must not dispense pseudoephedrine unless they are satisfied that the drug is being used for therapeutic needs. When pseudoephedrine is sold to a customer, the pharmacist must obtain the customer’s name and address, site an approved form of identification, and enter this into the log along with the amount of controlled drug sold. Any loss of stock—through accident, theft or misappropriation—must be immediately reported to the Pharmacy Board of Australia. Section 6 of the Drugs Misuse Regulation also imposes requirements upon a pharmacist when dispensing pseudoephedrine, similar to those outlined above. Section 6A of the Drugs Misuse Regulation requires the pharmacist to provide a copy of the documented information to the Police Commissioner.

Pharmacists have an ongoing obligation to maintain their professional development, and are required to obtain 40 Continuing Professional Development points each year. The main areas of focus for Continuing Professional Development points are improvement of knowledge and skills, and improvement in quality of practice. Pharmacists are expected to have a contemporary knowledge of drugs that are subject to abuse and misuse. They are taught to look for manipulative techniques of customers who are trying to obtain certain drugs. If they suspect that the drugs are being obtained for non-therapeutic purposes, then they have an obligation not to dispense them. Specifically, they are not to dispense more than one package containing pseudoephedrine unless exceptional circumstances exist.

Preventative measures

Although there is a requirement for pharmacists to log the sale of pseudoephedrine, this does not allow other pharmacists to see whether a customer has previously obtained pseudoephedrine from another pharmacist and when. This gap in preventative monitoring measures has led to the practice of ‘pharmacist-shopping’. Pharmacist-shopping occurs when individuals or groups who wish to obtain large quantities of pseudoephedrine visit different pharmacies to obtain the drug without raising suspicion.

An example of this type of pharmacist-shopping is illustrated in the matter of R v WR [2007] QCA 16. In that case, a truck driver was sentenced to a five-year term of imprisonment, to be suspended after two years, for an operational period of five years for trafficking and production of methylamphetamine. He received lesser concurrent terms for possession and other offences. In the unreported decision, Keane JA noted that:

The applicant also admitted to police that over a period of approximately 10 months between June 2002 and April 2003, he obtained approximately 500 boxes of pseudoephedrine, which he couriered
to other persons for the purpose of production of methylamphetamine. These tablets were purchased from many pharmacies in Queensland and New South Wales in the course of his occupation as a truck driver...

In 2004, reports from law enforcement agencies estimated 90 per cent of pseudoephedrine used in the making of illicit drugs was sourced from community pharmacies. The Queensland Branch of the Pharmacy Guild, in an effort to address this issue, developed Project STOP. Project STOP provides decision support to pharmacists who need to establish whether requests for pseudoephedrine-based products are legitimate. Using a computer program as an online tool, Project STOP tracks pseudoephedrine sales in real time. Project STOP operates in the following way:

- Upon receiving a request for a pseudoephedrine-based product, a pharmacist must ask to see photographic identification.
- The pharmacist must record the identification card number in a protected database operated by the Pharmacy Guild.
- The pharmacist must record the name of the product and the quantity requested.
- The database checks to see if the identification number has previously been entered into the database within an appropriate threshold period and flags any potential pharmacy-shopping or drug abuse/misuse.
- The pharmacist makes an informed decision whether or not to dispense the product and records the outcome.

The program also records instances when the database is opened but no information is entered, given the obvious concern of such conduct. When the system indicates that a customer has breached the threshold for requesting a pseudoephedrine-based product, a nominated police unit is automatically sent an alert and investigations are then made by the police. There are quarterly meetings between police, the Pharmacy Guild, and other stakeholders to discuss improvements and the efficacy of Project STOP. In 2007, the Australian Government supported the Pharmacy Guild of Australia in a nationwide roll-out of the Queensland-created program. Currently, 85 per cent of Queensland pharmacies use Project STOP.

There are costs associated with the use of Project STOP. The Commission has been advised that the cost associated with an annual subscription to Project STOP is $300 for non-Pharmacy Guild members; however, if the pharmacist is a guild member, the program is free.

The Queensland Police Service (QPS) advised the Commission on the policing benefits of Project STOP. Deputy Commissioner Ross Barnett confirmed that most pharmacists comply with their legislative requirement by using Project STOP to keep an online log of pseudoephedrine sold. Information received through Project STOP is viewed by the Chemical Diversion Desk, which is a unit attached to the State Drug Squad within the QPS. The Deputy Commissioner stated that information obtained from the Project STOP database can be a valuable intelligence tool, and is routinely used in drug investigations to validate other intelligence holdings. The Project STOP database can be used to identify a suspected offender’s patterns of movement and associates involved in the diversion of pseudoephedrine. A key to the success of the database is that it has the capacity to be used as a primary intelligence tool for generation of targets, and also as a secondary intelligence tool for corroboration of other intelligence. Since 2012, Project STOP has led to the generation of 135 intelligence reports.

In an interview with the Commission, Detective Inspector Mark Slater of the QPS Drug Squad noted the police intelligence function of Project STOP, but also spoke of its preventative effect. The restrictions imposed as a result of the use of Project STOP limits the amount of pseudoephedrine available to produce methylamphetamine in Queensland.

With the national roll-out of Project STOP and the consequential reduction in the availability of pseudoephedrine from local pharmacists for criminal purposes, the detections of unlawfully imported ContacNT (cold and flu medication known to contain a very high dose of pseudoephedrine) has increased...
significantly. Detections increased from 20.4 kilograms in 2009 to over one tonne in 2011-13. Whilst the program is available throughout Australia and is endorsed by the Pharmacy Guild of Australia, its use is not mandatory to those dispensing pseudoephedrine. As stated above, it is understood that currently 85 per cent of Queensland pharmacies use Project STOP.

While under state law, a pharmacist is required to keep a log in relation to the sale of pseudoephedrine that can be accessed online by the Commissioner of Police and the Director-General of Queensland Health, this is not as effective as Project STOP, which tracks the sale of pseudoephedrine in real time. Project STOP allows other pharmacists dispensing pseudoephedrine to access this sales information. A pharmacist who does not use this real-time database is limited in determining whether the purchase is for a legitimate therapeutic use. Further, in the absence of Project STOP, the police are not automatically alerted when a person has exceeded the allowable quantity.

Given the usefulness of this program for pharmacists—and the view of the QPS as to its effectiveness as a policing and preventative measure—the Commission queries why the program is not mandatory for those dispensing this very valuable and dangerous commodity, particularly given that the annual cost for a pharmacist who is not a Pharmacy Guild member is modest, and that it is free for Guild members.

The evidence of pharmacists aiding or enabling organised crime

The Commission sought advice from the Queensland Police Service, the Crime and Corruption Commission (CCC), and the Pharmacy Board of Australia as to whether those bodies had received any complaints or information within the last three years to suggest that chemists and/or pharmacists are directly or indirectly involved in the commission or facilitation of trafficking, supplying and/or producing a dangerous drug in Queensland.

The QPS advised that it was not in possession of any such information. The CCC advised that it was aware of one person who fit the criteria. Further inquiries revealed that the matter was currently proceeding before the courts. Accordingly, given the limitations of the Commission’s Terms of Reference, the Commission could not have further regard to that matter.

The Pharmacy Board of Australia provided a report to the Commission, listing notifications received about registered pharmacists and a synopsis of the matter and the outcome. Based on this list of notifications from the Pharmacy Board, the Commission examined relevant QCAT decisions since 2013 relating to disciplinary behaviour of pharmacists. Since 2013, there have been 11 reported decisions of QCAT where pharmacists have been found to have displayed behaviour amounting to unprofessional conduct or professional misconduct. All of these cases relate to pseudoephedrine-based products being dispensed contrary to guidelines and legislation. To enable an understanding of the way in which these pharmacists have facilitated drug offences, the summaries of a number of these cases are outlined below.

Case study

Pharmacy Board of Australia v Huynh

Mr Huynh was a registered pharmacist. In March 2008, he was convicted in the Supreme Court of Queensland of one count of producing dangerous drugs, namely, methylamphetamine. He was sentenced to two years imprisonment, to be suspended after six months, for an operational period of three years. A useful summary of the case against Mr Huynh can be found in the sentencing remarks of Justice Byrne, who stated:

Adam Huynh, you were between 29 and 32 years of age and conducting a business as a pharmacist when you committed the offence with which I am concerned and to which you have pleaded guilty
The illicit drug market

Queensland Organised Crime Commission of Inquiry

The unlawful production of the dangerous drug methylamphetamine between 1 January 2004 and 10 October 2006.

In that period, you sold to a covert police operative and others a quantity of pharmaceuticals typically, Telfast – containing a drug which to your knowledge could be, and in respect of the sales with which I am concerned you expected, would be used to produce methylamphetamine.

The covert police operative went to your pharmacy in Ipswich in September 2006 because you had purchased a very substantial quantity of Telfast from a manufacturer or wholesaler suspicious about the quantity of the drug.

The police operative was sold three packets of Telfast for $34.95 per packet – a mark-up of about 100 per cent on the ordinary retail price.

The operative asked for more boxes, and you arranged to supply him.

On the morning of 2 October 2006, the operative called you to confirm the purchase by him of 10 boxes. You said you had eight packets with you and expected more that morning.

The covert police operative said that he had 10 identity cards with him. You realised that they would be false or stolen and proposed to permit them to be used to facilitate the sale.

The police operative arranged to purchase another 10 boxes on the following Tuesday or Wednesday. He also asked you how to extract ephedrine from the pseudoephedrine in the tablets. You encouraged him to look up the process on the internet. Ten false or stolen IDs were to be used on that occasion, including IDs for women.

You declined to be interviewed.

The inflated prices suggest that you were engaging in these transactions to make money. The amount of money involved can only have been relatively small.

You said you were under some financial stress at the time in your business. Perhaps that is the explanation for the small amount of money you stood to gain by involving yourself in what you supposed was the manufacture and eventual sale of the drug, which as a pharmacist, you would have known only too well has a very significant potential for harm.

Pharmacists stand at the frontline. The community expects to rely upon their honesty, professionalism and compliance with the prescribed procedures to avoid the distribution into the criminal community of products containing pseudoephedrine.

A Pharmacist such as yourself who is tempted to facilitate this process must expect to go to prison if detected in such transactions. In a case such as this, general deterrence must assume appropriate significance.

An investigation was conducted by the Pharmacists’ Board of Queensland, where it was revealed that Mr Huynh sold approximately 1500 packets of pseudoephedrine-based product to a person known to be producing an illicit drug.39 It was estimated that 40 false identification cards were used to purchase the products.

Upon police investigations commencing in 2007, Mr Huynh provided an undertaking to the Pharmacists’ Board of Queensland that he would not practice as a pharmacist in any jurisdiction until the Board had completed any investigation. At the time of the hearing before QCAT, Mr Huynh had not practiced as a pharmacist for five and a half years. The Tribunal took this into account when making its final orders.

The Tribunal found that Mr Huynh acted in a manner which constituted unsatisfactory professional conduct. They ordered that he be ineligible to apply for registration for a period of one year. Upon being re-registered, Mr Huynh was also to be made subject to numerous conditions, involving continuing professional development and supervision for a period of two years.
Pharmacy Board of Australia v Arulogun

Mr Arulogun was a registered pharmacist. He owned and worked at a pharmacy he purchased in February 2010. A complaint was made to police by a staff member in April 2011 after 500 boxes of pseudoephedrine were ordered in one month, all of which were unaccounted for. In May 2011, Mr Arulogun was charged by police with supplying pseudoephedrine to a client, possessing methadone at his residential address, possessing pseudoephedrine at his address, and unlawful possession of a restricted drug. During a search of his home, police found 427 boxes of pseudoephedrine-based products.

The Australian Health Practitioner Regulation Agency launched an investigation into Mr Arulogun and information was gathered from colleagues revealing the extent of his unprofessional behaviour. Between January 2010 and February 2011, the pharmacy had purchased 379 boxes of pseudoephedrine products. In March 2011, 583 boxes had been purchased. Mr Arulogun was supplying large quantities of pseudoephedrine to a client. Staff recall seeing Mr Arulogun leaving the store with a black bag filled with pseudoephedrine products and meeting the client down the road to hand him the bag.

On 26 May 2011, the agency issued a notice to Mr Arulogun requesting employer details, inviting him to respond to the fact that he had been charged with four offences by police, and subsequently that he had failed to notify the Board within the prescribed time of seven days. On 31 May 2011, Mr Arulogun’s endorsement to dispense pseudoephedrine was cancelled. In June 2011, the Pharmacy Board of Australia placed Mr Arulogun on a number of conditions restricting his practice. Those conditions prohibited Mr Arulogun from obtaining, possessing, dispensing, prescribing, supplying or otherwise dealing with any products containing pseudoephedrine. He was further required to surrender any keys he had to access the pharmacy and was not to enter the pharmacy unless he was accompanied by a staff member.

It was revealed through ongoing investigations that Mr Arulogun had breached these conditions and was entering the pharmacy without staff being present, as well as accessing records relating to pseudoephedrine. In an attempt to legitimise the quantity of pseudoephedrine he was ordering, Mr Arulogun remotely accessed the pharmacy’s computer system and created false invoices for the sale of pseudoephedrine. When spoken to, each client claimed they had never bought pseudoephedrine from the pharmacy, with one client stating she was allergic to the drug. In October 2011, the Pharmacy Board of Australia placed further conditions on Mr Arulogun, preventing him from accessing any pharmacy records remotely or otherwise, as well as prohibiting him from entering the pharmacy under any condition.

Mr Arulogun pleaded guilty to amended charges in December 2011. He was convicted of six offences against the Health (Drugs and Poisons) Regulation, and three offences against the Drugs Misuse Act—namely, supplying a substance, possessing a dangerous drug and possessing a relevant thing. He was sentenced in January 2012 to 18 months imprisonment, with parole release after six months.

QCAT heard Mr Arulogun’s matter on 13 December 2013. In this time he had not practised as a pharmacist. The Tribunal found that Mr Arulogun:

...engaged in illegal conduct in order to make money. His excuse is that his pharmacy had lost business and he was under economic pressure. This hardly mitigates his criminal activity.

Plainly his conduct was of the kind that would assist to promote the manufacture of illicit drugs in the community and such conduct brings discredit to the pharmacy profession and betrays the public trust that pharmacists endeavour to preserve.
After his arrest the Board imposed various restrictions on him which he disregarded. This conduct was covert and continued over an extended period. QCAT found that Mr Arulogun had behaved in a way that constituted professional misconduct. Taking into account that he was no longer registered as a pharmacist, he was disqualified from being able to re-apply for registration for a period of two years.

**Case study**

**Pharmacy Board of Australia v Hung**

Mr Hung was a registered pharmacist. Between April 2010 and July 2010, he dispensed 1653 pseudoephedrine-based products. Mr Hung conceded to QCAT that he facilitated sales of this product that were inappropriate, and were in a volume and frequency beyond that which is necessary for therapeutic purposes. Mr Hung made some sales to customers whose names appeared on the Project STOP database as having previously been refused sale of pseudoephedrine-based products. Ultimately, Mr Hung accepted at the Tribunal that he ought to have known the pharmacy was being targeted by drug runners:

Mr Hung concedes that he facilitated sales of PSE that were inappropriate; they were in a volume and at a frequency beyond that necessary for therapeutic purposes. On 10 occasions over a 6-month period he dispensed multiple packs of PSE products. Some sales were made to customers where information contained on the online electronic database, Project STOP, revealed that other local pharmacies had denied sales to those persons. Mr Hung also concedes that he inappropriately dispensed PSE in that 5 of the customers who most frequently purchased PSE from the pharmacy did so in 2 groups; and there were a number of customers who repeatedly purchased or attempted to purchase PSE from the pharmacy on common dates and at times close together.

At all times when working in the pharmacy Mr Hung had available to him access to the pharmacy’s electronic dispensing database which included the patient’s record of purchases of PSE product. Mr Hung also had access to Project STOP. From that he would have been able to establish the patient’s PSE dispensing history from other pharmacies and whether he or she had been denied sales.

QCAT found that Mr Hung’s dispensing of pseudoephedrine-based products was repeated and inappropriate. Despite the behaviour of those purchasing these products being described as typical of groups of drug runners, it was held that Mr Hung’s relative inexperience as a pharmacist meant he was unable to detect this at first instance; however, he ought to have realised soon after the behaviour started. The Tribunal deemed that Mr Hung’s conduct amounted to unprofessional conduct. QCAT ordered him to be reprimanded, with conditions placed upon his registration. These conditions included Mr Hung being subject to six months of mentoring and further continuing professional development.

It is evident from the above cases that some pharmacy professionals have seriously breached the law. Such conduct by pharmacists can have substantial implications in the supply of precursor chemicals required to produce dangerous drugs. It is imperative that a clear message is sent to pseudoephedrine-dispensing pharmacists that, if they do so unlawfully, they will be dealt with severely—not only by law enforcement authorities, but also by their professional bodies. It is the view of the Commission that many of the penalties imposed upon these chemists are not severe enough to send this message, and that if the industry wants to put an end to such unlawful practices, the disciplinary consequences should be increased.
Conclusion

Pharmacists are heavily regulated, particularly with regard the dispensing of pseudoephedrine. However, despite such regulation, pharmacists are uniquely placed to enable organised crime and the production of illicit drugs, through the unlawful supply of precursor drugs or through poor dispensing practises. While the majority of pharmacists comply with their legislative requirements and voluntarily use Project STOP, the above examination of disciplinary hearings reveals that there are instances of pharmacists willing to use their position to unlawfully dispense pseudoephedrine.

It is imperative to send a clear message to the profession that the unlawful supply of pseudoephedrine will not be tolerated, that in disciplinary proceedings for actions such as these severe consequences must flow. It is the view of the Commission that the penalties to date have not been significant enough to send such a message.

The national roll-out of Project STOP has had a significant impact on the ability of criminals to obtain pseudoephedrine from pharmacists. Given the prevalence of methylamphetamine in the community and the dangers associated with using the drug, Project STOP is a critical initiative. The Commission understands that 85 per cent of Queensland pharmacies use Project STOP. While this is encouraging, it is the Commission’s view that such a critical initiative should be mandatory for all pharmacists. The cost associated with an annual subscription to Project STOP is modest: $300 for non-Pharmacy Guild members, and, if the pharmacist is a guild member, the program is free. 50 Making Project STOP mandatory would mean that all pharmacists and pharmacies in Queensland would have live and up-to-date access to a database designed to eliminate the abuse and misuse of pseudoephedrine-based products.

Recommendation

3.8 The Commission recommends that the Queensland Government legislate to make Project STOP mandatory for all pharmacies and pharmacists dispensing pseudoephedrine in Queensland. This may be achieved by inserting a provision in the Health (Drugs and Poisons) Regulation 1996.

(Endnotes)

4 Poisons Standard 2015 (Cth).
8 Section 55 Health Practitioner Regulation National Law Act 2009 (Qld).
9 Section 109 Health Practitioner Regulation National Law Act 2009 (Qld).
10 Section 130 Health Practitioner Regulation National Law Act 2009 (Qld).
12 Section 156 Health Practitioner Regulation National Law Act 2009 (Qld).
The illicit drug market

Queensland Organised Crime Commission of Inquiry

Section 196 Health Practitioner Regulation National Law Act 2009 (Qld).

Section 242(4) Health Practitioners (Professional Standards) Act 1999 (Qld).

Section 81A Health (Drugs and Poisons) Regulation 1996 (Qld).

Section 4A Health (Drugs and Poisons) Regulation 1996 (Qld).

Section 243 Health (Drugs and Poisons) Regulation 1996 (Qld).

Section 15 Health (Drugs and Poisons) Regulation 1996 (Qld).

Sections 86 & 129 Health (Drugs and Poisons) Regulation 1996 (Qld).

Section 285A Health (Drugs and Poisons) Regulation 1996 (Qld).

Section 277 Health (Drugs and Poisons) Regulation 1996 (Qld).

Sections 144 & 144A Health (Drugs and Poisons) Regulation 1996 (Qld).


Statutory declaration of Ross Barnett, 17 June 2015, paras 3–4 [In-Confidence].


Statutory declaration of Kathleen Florian, 4 June 2015, para 6.1 [In-Confidence].

Letter from Stephen Marty, Chair, Pharmacy Board of Australia, 11 June 2015.

Pharmacy Board of Australia v Adam Huynh [2013] QCAT 42 at [18]

Pharmacy Board of Australia v Adam Huynh [2013] QCAT 42 at [6]–[8].

Pharmacy Board of Australia v Arulogun [2013] QCAT 685 at [5]


Section 130(3)(a)(vii), Health Practitioner Regulation National Law Act 2009 (Qld).

Pharmacy Board of Australia, Schedule of Conditions, Mr Stephen Arulogun, PHA000969550.

Pharmacy Board of Australia, Schedule of Conditions, Mr Stephen Arulogun, PHA000969550.

Pharmacy Board of Australia v Arulogun [2013] QCAT 685 at [31]–[33].

Pharmacy Board of Australia v Hung [2014] QCAT 148 at [8].

Pharmacy Board of Australia v Hung [2014] QCAT 148 at [10].

Pharmacy Board of Australia v Hung [2014] QCAT 148 at [25].

Pharmacy Board of Australia v Hung [2014] QCAT 148 at [25].


Pharmacy Board of Australia v Hung [2014] QCAT 148 at [25].

Statutory declaration of Vanessa Law, 1 September 2015, p 2.
3.5.3 Lawyers

Introduction

The Commission’s Terms of Reference required the Commission to examine the role that lawyers may play in enabling or facilitating organised crime in Queensland. This part of the report particularly focuses on the role of lawyers in facilitating organised crime in the illicit drug market. Any role of lawyers in enabling money laundering is discussed in the money laundering chapter.

The Crime and Corruption Commission (CCC) advised this Commission that professional facilitators play a key role in helping criminal networks to operate undetected across both legitimate and illicit markets.1 Some facilitators are willing and are paid for their assistance, which they knowingly provide. Others may be entirely unaware they are, in fact, facilitating crime.2 Accountants and lawyers, for example, may be engaged because of their capacity to provide financial advice, to establish layered corporate structures, and to manage trust accounts. Such capabilities allow organised crime groups to launder the proceeds of crime, avoid tax, disguise criminal activity, avoid regulatory controls and frustrate law enforcement intervention.3

The Queensland Police Service (QPS) advised the Commission that organised crime enterprises may utilise professional and corporate structures, and engage the services of accountants, lawyers and financial experts to mask any illegal operations and to conceal illicit gains.4

Regulation for lawyers

The Supreme Court of Queensland governs the admission of lawyers to the roll of persons admitted as legal practitioners in Queensland. A legal practitioner is admitted to the Supreme Court of Queensland under section 35 of the Legal Profession Act 2007. Pursuant to that section, the court may make an order admitting the person if satisfied that they are eligible for admission and that they are a fit and proper person.

Before a person is entitled to practice in Queensland as either a solicitor or barrister, they must first apply to a relevant regulatory authority for a practising certificate.5 These regulatory authorities in Queensland are specified as being the Queensland Law Society (for solicitors) and the Bar Association of Queensland (for barristers).6

In addition to being subject to the provisions of the Legal Profession Act, there are specific rules that apply to solicitors and barristers in Queensland. Section 219 of the Act provides that the Law Society may make rules governing the practice of solicitors in Queensland. Section 220 of that Act also provides that the Bar Association may make rules about legal practice by barristers in Queensland.

Legal profession rules made by these bodies are binding on all Australian legal practitioners to whom they apply. Failure to comply with these rules can amount to unsatisfactory professional conduct or professional misconduct.7

As of 15 June 2015, there were 10,720 individuals holding current practising certificates issued by the Queensland Law Society, which authorised them to practice as solicitors in Queensland.

Is there evidence to suggest that lawyers are enabling organised crime in the illicit drug market?

The Commission required the QPS, the CCC, the Queensland Law Society, the Bar Association of Queensland and the Legal Services Commission to provide any information in their possession from the last three years that suggested or tended to suggest that solicitors and/or barristers were either directly or indirectly involved in the commission or facilitation of producing, supplying, or trafficking in a dangerous drug and/or laundering the monies obtained from the commission of such offences.

The Commission then conducted further investigations to establish whether any of the names referred to the Commission involved the lawyer acting in their professional capacity in relation to the offending conduct.
The QPS referred the Commission to a solicitor convicted of numerous offences of trafficking and supplying dangerous drugs. However, an examination of the case revealed that the offender did not use his role as a solicitor or his professional expertise to commit or facilitate the commission of the offences. The offender was a drug-dependent person who provided money to another person to purchase drugs for him, which he then both used himself and supplied to others. Therefore, the Commission did not view this offender as relevant to the Inquiry.

The QPS alerted the Commission to other matters that, at the time of the Inquiry, were subject to judicial proceedings. According to the Commission’s Terms of Reference, regard could not be had to such matters.  

Crime and Corruption Commission

The CCC referred the Commission to seven solicitors and one barrister who, in some way, may be involved in the commission of or the facilitation of producing, supplying, or trafficking in dangerous drugs and/or laundering monies obtained from the commission of the offences. However, of those matters, the Commission could not have regard to six cases because they were either subject to ongoing active and covert investigations, or they were connected with current proceedings.

Two matters involved finalised proceedings regarding two solicitors, one of which was the matter referred to the Commission by the QPS. The second matter involved a solicitor convicted of relevant drug offences; however, the facts of the case did not support a conclusion that he used his role as a solicitor or his professional expertise to commit or facilitate the commission of the offences.

Legal Services Commission

The Legal Services Commission referred the Commission to four solicitors charged with relevant drug offences. Of those matters, the Commission could not have regard to two cases because they were subject to current proceedings. The third matter was the same case referred by the QPS and the CCC. The fourth case was not concerned with drug offences and was not relevant to the Inquiry.

Bar Association of Queensland

The Chief Executive of the Bar Association of Queensland, Ms Robyn Martin, advised the Commission that the Bar Association was not aware of any conduct by any of its members relevant to the information sought.

Queensland Law Society

Mr Michael Fitzgerald, President of the Queensland Law Society, referred the Commission to four solicitors. Of those four solicitors, two are subject to current judicial proceedings (these are the same two as mentioned by the Legal Services Commission) and, accordingly, the Commission may not have further regard to them.

The remaining finalised matters have been discussed in relation to the matters referred by the QPS and the CCC.

Conclusion

On the evidence before it, the Commission has no reason to believe that solicitors or barristers in Queensland are using their profession or expertise to commit drug offences or to enable organised crime in the illicit drug market. It is accepted that there may be an ability for these professionals to be exploited through acts of money laundering, and this will be discussed in greater detail in the money laundering chapter.

(Endnotes)

1 Submission of the Crime and Corruption Commission, 22 May 2015, p. 34.
3.5.4 Violence and extortion

The Terms of Reference required the Commission to investigate the role violence and extortion plays in enabling or assisting organised crime.

In an Australian context, the public image of organised crime over the decades has been steeped in violence. The Melbourne gangland killings saw 36 members or associates from underworld groups killed during the period from 1998 to 2010.

Sydney has experienced its share of outlaw motorcycle gang violence. The Milperra Massacre, a gun battle between the Comancheros and the Bandidos in 1984, left seven dead, including a child. The violent and very public brawl in 2009 at the Sydney Airport between the Comancheros and Hells Angels saw one man beaten to death.

Queensland has also suffered violent conflicts between rival outlaw motorcycle gangs such as the ‘Ballroom Blitz’, a fight between the Finks and Hells Angels at a Gold Coast kickboxing tournament in 2006 involving guns and knives. It was in response to public violence between rival outlaw motorcycle gangs at Broadbeach on 27 September 2013, and a subsequent violent incident between police and members of the Bandidos the same evening, that the Newman Government announced its intention to crack down on criminal gangs, resulting in the introduction of controversial laws targeting criminal organisations, in particular, outlaw motorcycle gangs.

The Crime and Corruption Commission (CCC) advised this Commission\(^1\) that violence and extortion continues to be used by organised crime groups in Queensland as both a means to facilitate criminal activity and for financial gain. The CCC notes an increased use of violence by certain ethnic crime groups in Queensland in recent years and a move towards ‘gang- like’ behaviour. Certain younger ethnic crime entities in particular are attracted to gang culture and are more visible in their use of violence.

The CCC said that the most visible organised crime group involved in the use of violence and extortion in Queensland is outlaw motorcycle gangs. Violence is used to extort money and assets from legitimate business owners, non-affiliated drug dealers, rival gangs and people operating in gang territory. The outlaw motorcycle gang brand is heavily relied upon as a means to gain compliance for extortion demands. The CCC advised that there is evidence that violence for financial gain has become more brazen over time, particularly by younger members and associates who are willing to commit acts of violence in public, including using weapons, as a means of extorting cash and other commodities such as vehicles from victims.\(^2\)

The Queensland Police Service (QPS) advised the Commission that violence, including murder and extortion, have been key enablers used by outlaw motor cycle gangs to commit crime for many years. Such violence includes intimidation and harassment of, and violence towards, rival gangs and law enforcement officers carrying out their duties.\(^3\) The QPS refer to the 2012 Gold Coast shooting of a Bandidos member by a member of the Mongols as an example of extreme violence carried out by outlaw motorcycle gangs in public.

---

\(^1\) Statutory Declaration of Kathleen Florian, 4 June 2015, attachment 1 [In-Confidence].

\(^2\) Statutory Declaration of Paul Clauson, 4 June 2015, paras 2–3

\(^3\) Statutory Declaration of Robyn Martin, 3 June 2015, para 1.

\(^4\) Affidavit of Michael Fitzgerald, 11 June 2015.
The arrest statistics for Operation Resolute, the state-wide operation to address outlaw motorcycle gangs and serious crime activity across Queensland, provide some insight into the link between outlaw motorcycle gangs and violence.

As discussed in the chapter entitled ‘Outlaw motorcycle gangs’, statistics supplied by the QPS for arrests made under Operation Resolute reveal that such arrests account for only 0.52 per cent of arrests made across the state for alleged criminal conduct. What this shows is that outlaw motorcycle gang members account for a very small percentage of crime across the state. However, in examining the link between organised crime and violence as required by the Commission’s Terms of Reference, statistics relating to outlaw motorcycle gangs were the only relevant ‘organised crime’ statistics the QPS was able to provide to the Commission. The QPS advised the Commission that the statistics gathered by the Service ‘make it difficult to correlate between what is every day criminal activity and what could be identified as organised crime’.4

In response to information sought by the Commission, the QPS provided the arrest statistics5 for the period 1 October 2013 to 30 June 2015. On 696 occasions, outlaw motorcycle gang members were charged with offence/s. Of the 696 arrests of outlaw motorcycle members, 1093 charges were laid. Of those 1093 charges, 605 have been finalised by way of pleading guilty or a finding of guilt and 94 charges were finalised by way of acquittal or the prosecution offering no evidence. The remainder are yet to be finalised and are before the courts.

Of those 1093 charges, the Commission has analysed which of those offences have been charged under the Criminal Code and can be said to relate to violence and/or extortion. These are summarised below.

<table>
<thead>
<tr>
<th>Criminal Code (Qld) offence</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td>1</td>
</tr>
<tr>
<td>Grievous bodily harm</td>
<td>1</td>
</tr>
<tr>
<td>Unlawful wounding</td>
<td>1</td>
</tr>
<tr>
<td>Common assault</td>
<td>12</td>
</tr>
<tr>
<td>Assault occasioning bodily harm</td>
<td>14</td>
</tr>
<tr>
<td>Assault occasioning bodily harm whilst a vicious lawless associate</td>
<td>1</td>
</tr>
<tr>
<td>Assault occasioning bodily harm whilst armed and/or in company</td>
<td>12</td>
</tr>
<tr>
<td>Assault occasioning bodily harm whilst armed and/or in company whilst a vicious lawless associate</td>
<td>1</td>
</tr>
<tr>
<td>Assault occasioning bodily harm whilst armed and/or in company whilst a vicious lawless associate office bearer</td>
<td>2</td>
</tr>
<tr>
<td>Serious assault of a police officer</td>
<td>1</td>
</tr>
<tr>
<td>Serious assault of a person aiding a police officer</td>
<td>1</td>
</tr>
<tr>
<td>Serious assault of a police officer with a circumstance of aggravation</td>
<td>2</td>
</tr>
<tr>
<td>Serious assault of a police officer whilst pretending to be armed</td>
<td>2</td>
</tr>
</tbody>
</table>
### Criminal Code (Qld) offence

<table>
<thead>
<tr>
<th>Criminal Code (Qld) offence</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious assault of a person over the age of 60</td>
<td>1</td>
</tr>
<tr>
<td>Serious assault of a corrective services officer</td>
<td>1</td>
</tr>
<tr>
<td>Resist or obstruct police</td>
<td>2</td>
</tr>
<tr>
<td>Deprivation of liberty</td>
<td>2</td>
</tr>
<tr>
<td>Threats</td>
<td>3</td>
</tr>
<tr>
<td>Armed robbery in company and/or violence</td>
<td>2</td>
</tr>
<tr>
<td>Attempted armed robbery in company and/or violence</td>
<td>1</td>
</tr>
<tr>
<td>Extortion to gain a benefit</td>
<td>5</td>
</tr>
<tr>
<td>Extortion to gain a benefit whilst a vicious lawless associate</td>
<td>3</td>
</tr>
<tr>
<td>Extortion to gain a benefit with the threat of serious personal injury whilst a vicious lawless associate</td>
<td>2</td>
</tr>
<tr>
<td>Extortion with intent to cause detriment with threat</td>
<td>3</td>
</tr>
<tr>
<td>Riot</td>
<td>23</td>
</tr>
<tr>
<td>Going armed so as to cause fear</td>
<td>3</td>
</tr>
<tr>
<td>Affray</td>
<td>12</td>
</tr>
<tr>
<td>Affray whilst a participant in a criminal organisation</td>
<td>1</td>
</tr>
<tr>
<td>Threatening violence with words or conduct</td>
<td>1</td>
</tr>
<tr>
<td>Threatening violence by discharging a firearm</td>
<td>3</td>
</tr>
<tr>
<td>Threatening violence by discharging a firearm at night</td>
<td>1</td>
</tr>
</tbody>
</table>

### Criminal Code (Cth) offence

<table>
<thead>
<tr>
<th>Criminal Code (Cth) offence</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use carriage service to make threat to kill</td>
<td>3</td>
</tr>
<tr>
<td>Use carriage service to make threat to cause serious harm</td>
<td>1</td>
</tr>
<tr>
<td>Use carriage service to menace, harass or cause offence</td>
<td>3</td>
</tr>
</tbody>
</table>
Offences charged under the *Weapons Act 1990* and the *Explosives Act 1999* are relevant to note.

<table>
<thead>
<tr>
<th>Weapons Act offence</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful possession of weapons</td>
<td>8</td>
</tr>
<tr>
<td>Unlawful possession of weapons category D/H/R</td>
<td>13</td>
</tr>
<tr>
<td>Unlawful possession of weapons category D/H/R short firearm in public</td>
<td>1</td>
</tr>
<tr>
<td>Unlawful possession of weapons category C/E</td>
<td>1</td>
</tr>
<tr>
<td>Unlawful possession of weapons category A/B/M</td>
<td>11</td>
</tr>
<tr>
<td>Possession of knife in public place or school</td>
<td>12</td>
</tr>
<tr>
<td>Possess shortened firearms</td>
<td>1</td>
</tr>
<tr>
<td>Possess/acquire restricted items</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Explosives Act offence</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offence in relation to unauthorised and prohibited explosives</td>
<td>6</td>
</tr>
<tr>
<td>Authority required to possess explosives</td>
<td>14</td>
</tr>
<tr>
<td>Store explosives without authority</td>
<td>1</td>
</tr>
<tr>
<td>Unauthorised transport of explosives</td>
<td>1</td>
</tr>
</tbody>
</table>

**Extortion**

Queensland’s Criminal Code provides an offence of extortion which carries a maximum penalty of 14 years to life imprisonment, depending on the circumstances. The offence applies to a person who, without reasonable cause, makes a demand:

(a) with intent to—
   (i) gain a benefit for any person (whether or not the demander); or
   (ii) cause a detriment to any person other than the demander; and
(b) with a threat to cause a detriment to any person other than the demander; commits a crime.

The CCC advised this Commission that the number of extortion offences reported to the QPS rose sharply from 43 reported offences in 2011–2012 to 122 in 2013–2014. The CCC suspected, and the Commission shares the view, that the significant increase of reported extortions was due to the intense focus of police on outlaw motorcycle gangs under Operation Resolute and with the corresponding publicity, individuals feeling confident in reporting their complaints to police. Detective Inspector Michael Niland, of Taskforce Maxima, advised the Commission that with respect to violence and extortion associated with outlaw motorcycle gangs, most is unreported by the victims. Detective Inspector Niland noted that since the introduction of Taskforce Maxima, the number of reported offences increased substantially.
The Commission issued a notice to the QPS for copies of all QP9 summaries of facts in relation to extortion offences reported to the QPS in 2011/2012 and 2013/2014. The Commission only received copies of finalised matters. The Commission’s Terms of Reference prohibit the Commission from having regard to current proceedings before the courts. Of the 15 matters that the Commission could examine, it appeared on the facts of the QP9 summaries that there was little evidence of an element of organised crime involvement. Only two of the offences related to conduct by an alleged member of an outlaw motorcycle gang which could be said to be related to organised crime. The remainder of the offences were not organised or committed by organised criminal entities.

The Commission is aware that there are a large number of extortion offences currently proceeding before the courts where the allegation is that the offenders were either members, former members or associates of an outlaw motorcycle gang. As said, the Commission is unable to have regard to these matters.

Violence

Queensland’s Criminal Code provides strong maximum penalties for offences involving violence to person or property. The below outlines some of the violent offences and their maximum penalties.

**Riot**

If 12 or more persons who are present together: use or threaten to use unlawful violence to a person or property for a common purpose, and the conduct of them taken together would cause a person in the vicinity to reasonably fear for the person’s personal safety, each of the persons present commit the crime of riot. Riot simpliciter carries a maximum penalty of three years imprisonment. If the offender is armed or if property is damaged the offence carries seven years imprisonment. The offence carries life imprisonment for those who cause grievous bodily harm to a person, cause an explosive substance to explode or destroys or start to destroy a building, vehicle or machinery.

**Going armed so as to cause fear**

Any person who goes armed in public without a lawful reason and causes fear to any person commits the offence of going armed so as to cause fear. The maximum penalty for this offence is two years imprisonment.

**Threatening violence**

Any person who with an intent to annoy or intimidate any person, by words or conduct threatens to enter or damage a home or other premises, or with intent to alarm any person, fires a weapon or does any other act that is likely to cause any person in the vicinity to fear bodily harm or damage to property, commits the offence of threatening violence. If the offence is committed at night time, the maximum penalty is five years imprisonment. In all other circumstances the maximum penalty is two years imprisonment.

**Murder**

Any person who unlawfully kills another person, intending to kill or cause grievous bodily harm, is guilty of murder. The offence of murder carries mandatory life imprisonment with a mandatory minimum non-parole period of 20 years. The murder of a police officer carries a mandatory minimum non-parole period of 25 years and a 30 year non-parole period applies for multiple murder convictions. In Queensland, a life sentence means for the natural life of the person convicted. If they are granted parole, they will be on parole for the rest of their natural life.

**Conspiring to murder**

Any person who conspires with any other person to kill any person is guilty of a crime and liable to 14 years imprisonment.

**Manslaughter**

A person who unlawfully kills another under such circumstances as not to constitute murder is guilty of manslaughter. Manslaughter carries a maximum penalty of life imprisonment.
Unlawful striking causing death

A person who unlawfully strikes a person to the head or neck and causes the death of that person is guilty of the crime of unlawful striking causing death. The offence carries a maximum penalty of life imprisonment. The excuse of ‘accident’ is not available on this offence.

Acts intended to cause grievous bodily harm and other malicious acts

Any person who with intent to maim, disfigure or disable, to do some grievous bodily harm, or transmit a serious disease, in any way unlawfully wounds, does grievous bodily harm or transmits a serious disease to any person, commits the offence of acts intended to cause grievous bodily harm or other malicious act. The maximum penalty is life imprisonment.

Grievous bodily harm

Any person who unlawfully does grievous bodily harm to another is guilty of the crime of grievous bodily harm. The offence carries a maximum penalty of 14 years imprisonment. If the person is a participant of a criminal organisation and commits the offence on a police officer a mandatory minimum period of actual imprisonment for 12 months applies.

Torture

Any person who tortures another person commits the crime of torture. The term ‘torture’ is defined to mean the intentional infliction of severe pain or suffering on a person. The offence carries a maximum penalty of 14 years imprisonment.

Wounding

A person who unlawfully wounds another commits the offence of wounding carrying a maximum penalty of seven years imprisonment.

Common assault

Any person who unlawfully assaults another is guilty of common assault. The maximum penalty for common assault is three years imprisonment.

Assaults occasioning bodily harm

Any person who unlawfully assaults another and causes the other person bodily harm is guilty of assault occasioning bodily harm. If the person is armed or pretends to be armed or is in company with other persons, the maximum penalty is ten years imprisonment. In any other case the maximum penalty is seven years imprisonment.

Kidnapping

Any person who kidnaps another is guilty of a crime carrying a maximum penalty of seven years imprisonment. A person kidnaps another if the offender unlawfully and forcibly takes or detains the other person with intent to gain anything from any person or to procure an act or omission.

Kidnapping for ransom

Any person who takes, entices away or detains a person with the intent of extorting anything or procuring an act or omission, by a demand containing threats of detriment to the person kidnapped, is guilty of a crime carrying up to 14 years imprisonment depending on the circumstances.

Threats

Any person who threatens to cause a detriment to another with intent to prevent or hinder any person from doing a lawful act, or with intent to compel any person to do any act which the person is lawfully entitled to abstain from doing, or with intent to cause public alarm or anxiety, commits the offence of threats. The maximum penalty for this offence is ten years imprisonment if the threat is made to a law enforcement
officer, or a person helping a law enforcement officer when the officer is investigating the activities of a criminal organisation. In all other cases the maximum penalty is five years imprisonment.

**Robbery**

Any person who steals anything, and, at or immediately before or immediately after the time of stealing it, uses or threatens to use actual violence to any person or property in order to obtain the thing stolen or to prevent or overcome resistance to its being stolen, is guilty of robbery. If the person is armed or pretends to be armed, in company with other persons, wounds or uses other violence at the time of the robbery, the maximum penalty is life imprisonment. In any other case the maximum penalty is 14 years imprisonment.

**Demanding property with menaces with intent to steal**

Any person who, with intent to steal anything, demands it from any person with threats of any injury or detriment of any kind to be caused to the other person, either by the offender or by any other person if the demand is not complied with commits the offence of demanding property with menaces with an intent to steal. The maximum penalty is three years imprisonment.

**Arson**

Any person who wilfully and unlawfully sets fire to a building or structure, a motor vehicle, train, aircraft or vessel, any stack of cultivated vegetable produce, or of mineral or vegetable fuel, a mine, or the workings, fittings, or appliances of a mine is guilty of arson. The maximum penalty for arson is life imprisonment.

**Wilful damage**

Any person who wilfully and unlawfully destroys or damages any property is guilty of wilful damage. The maximum penalty for wilful damage simpliciter is five years imprisonment. However, aggravated penalties of seven years, 14 years and up to life imprisonment apply depending on the property damaged.

When examining the issue of organised crime and the use of violence, it is relevant to consider the offences and penalties in Queensland’s *Weapons Act 1990*:

**Possession of weapons**

Any person who unlawfully possess a weapon is guilty of an offence. The maximum penalties range from two years to 13 years imprisonment depending upon the number, and category of weapon. If the person uses a firearm in the commission of an indictable offence, they must be sentenced to a mandatory minimum of nine months to 18 months imprisonment (depending on number and category of weapon) to be served in its entirety. If the person possesses a firearm for the purpose of committing an indictable offence, or possesses a shortened firearm in a public place, they must be sentenced to a mandatory minimum of six months to 12 months imprisonment (depending on number and category of weapon) to be served wholly in a correctional facility.

**Unlawful supply of weapons**

Any person who unlawfully supplies a weapon to another person is guilty of an offence. The maximum penalties range from four years to 13 years imprisonment depending on the number and type of weapon. If the person supplies a shortened firearm, they must serve a mandatory minimum of two and half years to three years imprisonment (depending on the number and category of weapon).

**Shortening firearms**

Any person who, without reasonable excuse, shortens a firearm, possesses a shortened firearm, or acquires or sells a shortened firearm, is guilty of an offence. The maximum penalty for this offence is four years imprisonment.
The illicit drug market

A person who unlawfully carries on the business of trafficking in weapons or explosives commits a crime. The offence carries a maximum penalty of 15 years to 20 years imprisonment depending on the category of weapon. A mandatory minimum period of three and half years to five years imprisonment applies where at least one of the weapons trafficked is a firearm and depending on the category of firearm.

Sentencing

Penalties and Sentences Act 1992

The Penalties and Sentences Act 1992 provides a broad range of sentencing options for the courts to impose appropriate sentences in order to punish and rehabilitate offenders, deter offenders or other persons from committing similar acts, denounce the criminal conduct and protect the Queensland community.

With regards to offences of violence, the Penalties and Sentences Act provides a special sentencing regime for offenders convicted of serious violent offences. The regime is provided in part 9A and applies to offences listed in schedule 1 of the Act. Offences in schedule 1 of the Act include (prescribed offences) – riot, threatening violence, conspiring to murder, manslaughter, acts intended to cause grievous bodily harm and other malicious acts, grievous bodily harm, torture, wounding, assaults occasioning bodily harm, kidnapping, kidnapping for ransom and robbery.

If an offender is declared by the court to be convicted of a serious violent offence, the offender must serve 80 per cent of their term of imprisonment before being eligible to apply for parole. An offender convicted of a prescribed offence and who is sentenced to 10 or more years imprisonment must be declared to be convicted of a serious violent offence. The court has a discretion to declare an offender to be convicted of a serious violent offence if the court imposed a term of imprisonment of five or more, but less than 10, years imprisonment.

Vicious Lawless Association Disestablishment Act 2013

When examining the issue of organised crime and the use of violence, regard must be had to the Vicious Lawless Association Disestablishment Act 2013 (VLAD Act).

The VLAD Act provides a legislative scheme where members of criminal associations that commit serious criminal activity for the purposes of, or in the course of participating in the affairs of the relevant association, are subject to significant mandatory terms of imprisonment. These terms range from 15 years to 25 years, and are in addition to the penalty which a court imposes for the original offending behaviour. This sentence is to be cumulative upon any other sentence imposed and must be served wholly in a corrective services facility. The person is not eligible for parole at all throughout this sentence. The penalty may only be reduced in particular circumstances where the person undertakes to cooperate with law enforcement authorities and that offer is accepted by the Commissioner of Police.

The QPS advised the Commission that between 1 October 2013 to 30 June 2015, 65 persons were charged with an offence where the circumstance of aggravation that the person is a vicious lawless associate under the VLAD Act was alleged. If proven, the circumstance of aggravation mandates the imposition of an additional 15 years imprisonment, cumulative to the term of imprisonment imposed for the substantive offence.

Further, during that period, 36 persons were charged with an offence/offences where the circumstance of aggravation of being a vicious lawless associate was alleged with a further VLAD Act circumstance of aggravation of being an officer bearer. If proven, the ‘office bearer’ circumstance of aggravation mandates a further 10 year term of imprisonment, cumulative to the 15 year term for being a vicious lawless associate and cumulative to the term of imprisonment imposed for the substantive offence. Therefore, if a person is convicted of being a vicious lawless associate with the circumstance of aggravation of being an officer bearer, the person will receive 25 years imprisonment cumulative to the term of imprisonment imposed for the substantive offence.
While there have been a number of persons charged with the circumstances of aggravation of being a vicious lawless associate, as of 18 September 2015, only one person had been so convicted. That person was not deemed a vicious lawless associate due to his involvement with any outlaw motorcycle gang, but rather due to him being one of a group of four who were involved in the commission of various drug offences, including declared offences under the Act. That person ultimately cooperated with the authorities, and received a significantly reduced sentence as a result of that cooperation. Detective Inspector Niland of Taskforce Maxima in the QPS noted that the offender’s cooperation had a significant impact on the network he was involved in. He stated that a positive aspect of the legislation is that it provides defendants with a great incentive to cooperate with authorities, given the dire consequences that will mandatorily flow as a result of conviction of this circumstance of aggravation. Instances of persons charged with this circumstance of aggravation are now being adjourned awaiting the finalisation of this Inquiry and the Government’s Taskforce. It is clear to the Commission that certainty needs to be provided as to the whether the current laws will remain in order to allow proceedings to be finalised.

Conclusion

The CCC advised this Commission\(^42\) that violence and extortion continues to be used by organised crime groups in Queensland as both a means to facilitate criminal activity and for financial gain. The CCC said that the most visible organised crime group involved in the use of violence and extortion in Queensland is outlaw motorcycle gangs. Violence is used to extort money and assets from legitimate business owners, non-affiliated drug dealers, rival gangs and people operating in gang territory. The outlaw motorcycle gang brand is heavily relied upon as a means to gain compliance for extortion demands.

The QPS advised the Commission that violence, including murder and extortion, has been a key enabler used by outlaw motorcycle gangs to commit crime for many years. Such violence includes intimidation and harassment of, and violence towards, rival gangs and law enforcement officers carrying out their duties.\(^43\)

However, the information provided to the Commission and to which the Commission could have regard under its Terms of Reference evidencing a link between organised crime and violence and extortion was very limited. The QPS advised the Commission that the statistics gathered by the Service ‘make it difficult to correlate between what is every day criminal activity and what could be identified as organised crime’.\(^44\) The Commission did receive arrest statistics for Operation Resolute from the QPS which were of limited assistance. The statistics revealed outlaw motorcycle gang members account for a very small percentage of crime across the state, 0.52 per cent in fact. Some of those arrests concerned offences of violence or were violence-related, however, the statistics themselves do not show whether the violent conduct was in any way related to the person’s membership of an outlaw motorcycle gang.

With regards to charges for extortion, the Commission notes the sharp rise in reported extortion offences since the commencement of Operation Resolute. The Commission’s Terms of Reference limited the Commission in the number of extortion matters it could examine. However, of those examined there was little evidence of an element of organised crime involvement. While there are a number of cases before the courts that do allege organised crime involvement, these cases are not finalised and the evidence has not been tested. Accordingly, no conclusions can be drawn from those cases as to the role of organised crime.

The Commission of course accepts the advice of the CCC and the QPS that organised crime groups and in particular, outlaw motorcycle gangs are ready and willing to use violence and extortion to achieve their criminal activities.

The Commission also accepts that many offences of violence and extortion go unreported because of the very nature of that type of conduct. Many of the victims of these types of crimes are in fear for their personal safety and the safety of those around them, and as such are more reluctant to make a complaint to the authorities. Accordingly, it is unsurprising that the number of cases both reported and finalised before the courts is limited.
While the Commission accepts these assertions, it is important that law enforcement agencies maintain a holistic approach to organised crime in Queensland. The Commission’s view is that disproportionate attention has been given to outlaw motorcycle gangs since October 2013.

(Endnotes)

1 Submission of Crime and Corruption Commission, 22 May 2015, p. 31.
6 Section 415 of the Criminal Code.
8 Submission of Crime and Corruption Commission, 22 May 2015, p. 32.
9 Transcript of Interview, Michael Niland, 2 July 2015.
10 Notice to produce documents, Queensland Police Service, 4 June 2015.
11 Section 61 Criminal Code.
12 Section 69 Criminal Code.
13 Section 75 Criminal Code.
14 Sections 302 & 305 Criminal Code.
15 Section 309 Criminal Code.
16 Sections 303 and 310 Criminal Code.
17 Section 314A Criminal Code.
18 Section 23(1)(b) Criminal Code.
19 Section 317 Criminal Code.
20 Section 320 Criminal Code.
21 Section 320A Criminal Code.
22 Section 323 Criminal Code.
23 Section 335 Criminal Code.
24 Section 339 Criminal Code.
25 Section 354 Criminal Code.
26 Section 354A Criminal Code.
27 Section 359 Criminal Code.
28 Sections 409 & 411 Criminal Code.
29 Section 414 Criminal Code.
30 Section 461 Criminal Code.
31 Section 469 Criminal Code.
32 Section 50 Weapons Act.
33 Section 50B Weapons Act.
34 Section 61 Weapons Act.
35 Section 65 Weapons Act.
36 Section 9 Penalties and Sentences Act 1992.
37 Sections 7 & 8, Vicious Lawless Association Disestablishment Act 2013 (Qld).
40 Statutory declaration of Michael Byrne QC, 27 August 2015.
41 Transcript of Interview, Michael Niland, 2 July 2015, p. 12 [In-Confidence].
3.6 Responses to organised crime

Organised crime groups in Queensland are developing in ways that mirror large corporations. These developments include the centralisation of operations, greater connectivity, growing sophistication, increased professionalism, and long term strategic planning geared towards growth. This is leading to more sophisticated criminal activities, broader criminal networks, and groups with greater capabilities. As a result, multi-jurisdictional offending is increasing with overseas and interstate-based crime groups targeting Queensland and Queensland-based crime groups expanding their operations interstate and overseas.¹

The ability of law enforcement to effectively impact on organised crime is beyond the scope and capability of any one agency. Collaborative national and interstate arrangements are essential.²

3.6.1 Queensland Police Service

The Queensland Police Service (QPS) response to organised crime is a two-pronged approach. First, intelligence-based tactical approaches are used at a local level and nationally through joint taskforces and operations. Second, the QPS focus on preventative strategies such as education and community engagement.³

Local level

Local policing plays an integral role in combatting organised crime. QPS officers enter observations and findings every day into the QPS data collection system which is shared nationally through the CrimTrac Agency in Canberra.⁴ Approximately 65,000 law enforcement officers and personnel across Australia access CrimTrac systems on a daily basis. QPS officers are responsible for approximately 2.6 million searches on the CrimTrac National Police Reference System annually.⁵ This information-sharing technology allows local, frontline police officers to access information which may potentially link organised crime activities from far-reaching corners of Australia to Queensland.

The QPS has established a network of policing groups designed to work in an integrated fashion to best tackle organised crime and drugs within the state. The Drug and Serious Crime Group commenced on 1 July 2013. The Drug and Serious Crime Group focuses on protracted operations against high level organised crime networks beyond the scope and capacity of individual local criminal investigation branches.⁶ Within the Group are several other units. The Commission sought information from the QPS as to the resourcing attached to the units.

The Commission was provided with the number of police officers attached to the Drug and Serious Crime Group as at 24 August 2015. The Commission was also provided with the number of police officers usually attached to the Drug and Serious Crime Group but that were on secondment as at that date.⁷ This information disclosed that as of 24 August 2015, 28 per cent of the police officers attached to the Drug and Serious Crime Group were on secondment.

The QPS insisted on maintaining a claim for confidentiality regarding the Commission disclosing the precise numbers of police officers engaged with relevant taskforces, including the Drug and Serious Crime Group.

The Commission had regard to the number of police officers assigned to Taskforce Maxima: the taskforce created to eradicate outlaw motorcycle gangs.⁸ While the Commission was cognisant of the QPS claim for confidentiality, it noted that the number of police officers assigned to Taskforce Maxima has been publicly reported in the media. For example, the Sunshine Coast Daily reported earlier this year that the Taskforce is comprised of 90 officers.⁹ While not exact, the publicly reported number is within the range of the figure provided to the Commission.
While the Commission cannot report on the precise number of officers assigned to drug investigations, when compared to those attached to Taskforce Maxima, the Commission found the allocation of resources difficult to reconcile, particularly given that outlaw motorcycle gang members account for 0.52 per cent of persons charged with criminal offences throughout Queensland, and given the prevalence and impacts of the illicit drug market.

As recommended in a previous chapter on outlaw motorcycle gangs, it is the Commission’s view that the QPS focus its policing strategies beyond outlaw motorcycle gangs to other areas of organised crime that pose a risk to Queensland.

The State Drug Squad focuses on trafficking and production of dangerous drugs. The Organised Crime Investigation Unit concentrates on organised crime activity throughout the state. In addition to these units, the Townsville and Cairns Drug Squads focus on northern Queensland criminal activity. Finally, the Gold Coast Major and Organised Crime Squad targets significant criminal organisations committing offences on the Gold Coast and South East Queensland region, including major drug trafficking and production. All of these units operate under the Drug and Serious Crime Group.10

The State Drug Squad comprises several units including the Protracted Operations Unit, Drug Taskforce, Taskforce Backstay and the Synthetic Drug Operations Unit. A Firearms and Cultivated Team, although not a unit within the State Drug Squad, is a further unit within the Organised Crime Investigation Unit and which has some involvement in drug investigations. The charter of the Firearms and Cultivated Team is to investigate major and organised crime elements involved in firearms trafficking and cannabis productions.11

The Protracted Operations Unit and Drug Taskforce focus primarily on major protracted operations targeting the higher-end criminal networks involved in drug production and trafficking. Taskforce Backstay is engaged in a similar-styled protracted operation targeting Asian crime syndicates. The taskforce is engaged in a multi-agency operation targeting drug importation and trafficking in the Brisbane area.12

The QPS has a Chemical Diversion Team dedicated to looking at emerging trends with illicit substances and researching within Australia and overseas. The team operates within the Synthetic Drug Operations Unit13 and looks into suspicious deaths that may be linked to emerging substances and then follows the matter through to any Coronial Inquest. If it is determined the substance is dangerous and has not been classified in the Drugs Misuse Regulation, a recommendation can be made.14 The Chemical Diversion Team also participates in state and national forums to enhance drug policy and reform.15

The Illicit Laboratory Investigation Team also works within the Synthetic Drug Operations Unit and is responsible for attending and processing clandestine illicit drug laboratories across Queensland. The Townsville and Cairns Drug Squads also perform functions in this area. The Illicit Laboratory Investigation Team is also responsible for investigating major and organised drug production. The volume of drug laboratories detected in Queensland on an annual basis results in minimal major investigations by the Illicit Laboratory Investigation Team; however, they are involved in state-wide training in lab awareness and handling procedures.16

The work undertaken by the Drug and Serious Crime Group is crucial to the prevention and investigation of serious crime in Queensland. The QPS advised the Commission that 76 per cent (an indicative percentage only) of identified Queensland organised crime networks are involved in the illicit drug market.17 It is therefore imperative that this Group is sufficiently resourced to combat organised crime in the drug industry in Queensland.

**National and international level**

Operation Resolute oversees all activity to address outlaw motorcycle gangs and serious crime activity across Queensland through Taskforces Maxima and Takeback. Taskforce Maxima targets outlaw motorcycle gang’s unexplained wealth and criminal business activities, whereas Taskforce Takeback adopts a high-visibility approach to policing acts of public violence and intimidation on the Gold Coast.18
In addition to covert and tactical strategies employed by Maxima, an emphasis has been placed on building relationships with other state, national and international counterparts. These relationships were furthered in April 2014, when the National Anti-Gangs Squad was relocated to QPS headquarters in Brisbane to work alongside Maxima in the national fight against organised crime.19

The National Anti-Gangs Squad was established in 2013 as a federal government initiative in the fight against organised crime. The Squad is made up of members from the Australian Federal Police (AFP), state police forces, Australian Crime Commission (ACC), Australian Taxation Office, Australian Customs and Border Protection Service, Department of Immigration and Border Protection and the Department of Human Services. The Squad operates on a national level to support local strike teams in each state and territory. The Squad aims to detect, deter and disrupt gang related crime in Australia through collaboration with their relevant partners. The National Anti-Gangs Squad is able to enhance the capability of state and territory law enforcement agencies to fight gang-related activity by providing coordinated investigative, intelligence, technical and asset confiscation support.20 Information and intelligence are gathered and disseminated across Australia. The flow of information works in reverse as well, from strike teams back to the national body.21 The QPS has participated in the National Anti-Gangs Squad since the Squad’s relocation to QPS headquarters.22

The diagram below outlines the flow of information, coordination and cooperation.23

An example of benefits flowing from cooperation between agencies can be seen in the detection of imported illicit drugs. The QPS works closely with the AFP and the Australian Customs and Border Protection Service to intercept illicit drugs being sent to Queensland through the mail. The AFP has established a rapid lab at the Sydney Mail Exchange where all mail entering Australia is processed. This allows a centralized point wherein illicit substances can be targeted.24

One of the key requirements for law enforcement agencies to combat organised crime is intelligence services. The State Intelligence Group is responsible for the delivery of intelligence services to the QPS and other stakeholders. The provision of intelligence aides supports decision making at tactical, operational and strategic levels.25 In order to successfully provide these services, QPS has stationed intelligence officers
The illicit drug market throughout Queensland to allow a geographically expansive approach. The State Intelligence Group is responsible for information collection, collation, analysis and dissemination of intelligence products with the QPS, Australia and internationally.

In recognition of the ability for organised crime to transcend borders and flow into a problem shared by each state and territory within Australia, the National Organised Crime Response Plan (NOCRCP) 2010–2013 was developed by the Commonwealth. The success of this plan led to the development of the 2015–2018 Plan. The National Organised Crime Response Plan sets out the high-level policy approach to responding to organised crime within Australia.26 There is an emphasis within the Plan on improving cross jurisdictional operability and information sharing, targeting the criminal economy, improving operations responses and preventative strategies, as well as improving domestic, national and international partnerships.27

The NOCRP assists the States and the Commonwealth to align priorities and promote collaborative and cohesive arrangements between the two, which underpin a national response to organised crime.28

Despite an emphasis on aligning priorities and promoting a collaborative approach, the National Organised Crime Response Plan recognises that each state and territory is best placed to combat organised crime within their legislative framework, and accommodates this while preserving a role for the Commonwealth as well.29

The QPS Operational Plan 2014–15 identifies at the operational level a range of organised crime related activities for focus in the forward period which are aligned to the NOCRP, including working closely with Commonwealth law enforcement and intelligence agencies and targeting high level individual and network criminal activities. These and other activities contribute the overall performance of the QPS across a range of crime related areas, of which organised crime is one and reflects the full broader ambit of policing responsibilities.31

However, when investigating organised crime, the QPS has established important partnerships with state and national agencies. Within Queensland, the CCC works closely with the QPS in fighting organised crime and investigates specific areas of major crime.32

The information gained from these agencies allows the QPS to have a holistic approach to organised crime prevention.33

The QPS, through the State Drug Squad and Chemical Diversion Team, is involved in making submissions to various national forums to help combat organised crime and the illicit drug market. The recently formed National Ice Taskforce is one of the groups QPS work closely with.34

The National Drug Strategy is an overarching strategy which promotes a consistent approach to tackling the illicit drug trade throughout the country. In an interview with the Commission, Detective Inspector Mark Slater stated that the National Drug Strategy does not form the basis of policing methods; however, it guides the QPS with broad parameters on what policing methods and targets may be presently relevant to Queensland. Detective Inspector Slater went on to say that the current focus was the drug ice. However, the Detective Inspector said attention to other drugs was not lost, as a holistic approach to fighting the illicit drug trade is required. The QPS is cognisant of the fact that if it focuses too heavily on one area of the market, another area will emerge as a problem.35

The QPS works in conjunction with the ACC and benefits from the ACC’s specialist analytical capabilities and ability to undertake operations unable to be performed by local policing agencies. Working in unison with the ACC, the QPS is able to meaningfully contribute to the National Organised Crime Response Plan, focusing on cross jurisdictional threats from organised crime groups.36

The Serious and Organised Crime Coordination Committee is a national body represented by all states and territory law enforcement agencies, the Australian Customs and Border Protection Service and the Australian Taxation Office. Its primary objective is to assist in the coordination of a national response to organised crime. In addition to this, the Australian Criminal Intelligence Forum brings together intelligence and law enforcement agencies from across Australia and New Zealand to foster a relationship of information and intelligence-sharing.37
In additional to large national bodies, a number of state- and territory-based intelligence forums at the tactical level have been established with a common, national purpose. Referred to as Joint Analyst Groups, the primary goal is to identify, coordinate and prioritise target intelligence and management as well as supporting local decision-making. The Queensland branch of the national initiative was established permanently in May 2015 and focuses on identifying high value organised crime networks.

The benefits of a cross-jurisdictional approach to combating organised crime are best evidenced by the National Crime Target List. The ACC holds the National Crime Target List which identifies organised crime risks, including nationally significant syndicates and individuals impacting Australia. This material is distributed to law enforcement which facilitates operational priorities (for example, Queensland currently has over 100 targets listed on the National Crime Target List). The QPS is also made aware of new intelligence through the List, assisting in the state-wide analysis of organised crime, allowing police to gauge the potential impact of organised crime groups on Queensland.

It can be seen that the QPS is actively responding to the major threat that illicit drugs pose to Queensland. This has been done both by policing at a local level and through interaction with other state and federal bodies. Such a national and cross-jurisdictional approach is vital as the illicit drug market is a borderless trade.

Care must be taken, however, to ensure that the QPS is sufficiently resourced to deal with the significant problem of illicit drugs. The QPS did not assert to the Commission that it was under-resourced in this area. What is evident to the Commission is that a significant amount of QPS resources has been channelled into addressing outlaw motorcycle gangs in circumstances where members of such gangs account for a very small percentage of crime in this state. The establishment of the Ice Taskforce and the Commonwealth Government’s ‘Dob-in-a-Dealer’ campaign may necessitate the reallocation of resources within the QPS to ensure that new information can be appropriately investigated. Public confidence in the Taskforce, campaign, and the QPS must not be eroded by an inability to properly respond to and investigate information and intelligence gained.

### 3.6.2 Crime and Corruption Commission

The Crime and Corruption Commission’s (CCC) objectives are to reduce the impact of major crime, reduce the incidence of serious corruption in the public sector and provide an effective witness protection service. The CCC is a statutory body and its functions and powers are set out in the Crime and Corruption Act 2001. The CCC’s scope of investigative powers allows it to investigate matters pertaining to the general community in Queensland, the public sector, police and witnesses. In summary, the CCC:

- investigates organised crime, paedophilia, terrorist activity and other serious crime referred to it for investigation
- receives and investigates allegations of serious or systematic corrupt conduct
- helps in the recovery of proceeds of crime
- provides the witness protection service for the state of Queensland
- conducts research on crime, policing or other relevant matters.

The Crime and Corruption Act recognises the need for a multi-agency approach to combat major crime, and it allows the CCC to provide information to, and receive information from, other law enforcement agencies and prosecuting authorities, including entities outside Queensland. The CCC works closely with relevant agencies, sharing intelligence products, operational resources and participating in joint investigations.

The CCC plays an important role in the fight against organised crime and drugs in Queensland. It has the ability to gather strategic intelligence against organised crime entities involved in the illicit drug trade. Teams within the CCC use different areas of expertise including forensic computing, information technology, forensic accounting, surveillance techniques and human sources. This enables the CCC to focus its...
attention on specific targets involved in organised crime drug markets, based on evidence obtained using their multi-disciplinary teams. The CCC may make arrangements with the QPS to establish special taskforces to assist in the investigation of organised crime.\textsuperscript{45}

As at 25 August 2015, there were 85 QPS officers currently seconded to the CCC in various positions.\textsuperscript{46} Of those officers, ten are assigned to the investigation of organised crime and illicit drug use. These officers came from various areas within the QPS, including the State Drug Squad, Tactical Crime Squad, Homicide Squad and Ethical Standards Command.\textsuperscript{47} Other seconded QPS officers assist in physical surveillance, technical surveillance, forensic computing, police command and witness protection.\textsuperscript{48}

The CCC regularly reviews the illicit drug market and its associated risks. From this assessment, an annual Drug and Commodities Guide is published. This document provides a general overview of the most accessible drugs in Queensland and their various prices to allow law enforcement agencies within the state to implement appropriate operational policing methods.\textsuperscript{49} The CCC also focuses its operational activities on those high-risk areas. In recent years, those areas have involved methylamphetamine and cocaine.\textsuperscript{50}

The CCC works in conjunction with the QPS, AFP, ACC, AUSTRAC, Australian Customs and Border Protection Service, and the Australian Taxation Office, and participates in a framework of law enforcement forums that are overseen by the Queensland Joint Management Group.\textsuperscript{51} The forums resulting from this Group and overseen by the Queensland Joint Management Group are:

- Queensland Operations and Coordination Group
- Queensland Joint Analyst Group Committee
- Queensland Joint Analyst Group Practitioners
- Queensland Serious Financial Crime Group.\textsuperscript{52}

The focus of this framework of law-enforcement forums is to coordinate multi-agency activities around organised crime in Queensland to ensure that:

- there is a shared view of serious and organised crime threats in Queensland
- there is a multi-agency commitment to the identification of serious and organised crime threats and risks
- there is a multi-agency commitment to the intelligence development of the most serious threats
- serious and organised crime operational activity engaged in by all members is de-conflicted
- where appropriate, agencies come together to address serious and organised crime threats
- agencies collaborate to develop multi-agency capabilities and shared learning and development opportunities.\textsuperscript{53}

The CCC conducts strategic intelligence assessment of organised crime activity within Queensland every three to five years. Among other areas, the illicit drug market is targeted. The Intelligence Development Unit collects intelligence from a wide range of sources, allowing the CCC to be well-informed when conducting these assessments and allowing for a better-informed Queensland.\textsuperscript{54} This information is also shared with the ACC.

Intelligence collection priorities are developed through the Crime Market Assessment Process and updated regularly. The CCC monitors the national and state-based organised crime networks to allow for more accurate intelligence collection priorities. This is used to help with decision-making and resource allocation to ensure the highest threat targets are investigated.\textsuperscript{55} The CCC combines intelligence collection priorities with Target Risk Assessment Methodology, a nationally agreed consistent methodology ranking targets, to ensure the correct criminal organisations groups are targeted based on the most up-to-date risk assessment.\textsuperscript{56}

Once organised crime groups have been targeted, the CCC develops a unique response based on the threat posed. A protracted investigation may take place, requiring a high level of physical and technical surveillance and which may be very resource intensive. Shorter operations aimed at disrupting an organised crime group may also be undertaken. These are often used for high-risk markets that pose a significant and immediate threat to the community such as the methylamphetamine market.\textsuperscript{57}
One of the major strengths of the CCC is its ability to use coercive hearings to obtain new information and evidence.58 This type of hearing allows the Commission to assist other agencies, including the QPS, to further investigations that have reached a point of stagnation.59 The CCC becomes involved in QPS matters when a referral is made and considered by the Crime Reference Committee.60 General referrals are used for organised crime involving the illicit drug market.

Unlike regular court hearings, witnesses called to CCC hearings must answer all questions put to them. The right to silence in the case of self-incrimination is not available, and refusal to answer questions can lead to charges which carry custodial sentences.61 The CCC has used these powers to gain invaluable intelligence regarding organised crime and drug trafficking networks in Queensland.

The CCC also assists in the fight against organised crime and the illicit drug trade by informing the Queensland public about emerging trends and key investigative findings. Declassified intelligence and research reports are published to inform the community of current issues in law enforcement and crime prevention, including illicit drug markets in Queensland.62

3.6.3 Office of the Director of Public Prosecutions

The Director of Public Prosecutions and staff have the primary function of prosecuting (on behalf of the State of Queensland) criminal matters in the High Court of Australia, Court of Appeal, Supreme Court, District Court, Childrens Court, Magistrates Court and Mental Health Court. The Office of the Director of Public Prosecutions (ODPP) also helps victims of crime and their families deal with their interaction with the criminal justice system, primarily through the provision of information on court events and referral services. In addition, the ODPP, in conjunction with the CCC, has a role in restraining and confiscating proceeds of crime under the relevant legislation dealing with the confiscation of criminal proceeds.63

In its submission to the Commission, the Acting Director of Public Prosecutions, Mr Michael Byrne QC, stated that the primary role that the ODPP has in preventing and combating any crime is ensuring that criminal prosecutions are conducted as effectively as possible where there are reasonable prospects of conviction. The role of the prosecutor in criminal proceedings is attended by considerations of impartiality and the obligation to fully and fairly present all relevant evidence to the Court.64 As to the effectiveness of the ODPP, statistics relating to a three-year period of financial years 2010/11 to 2013/14 showed that between 86.4 per cent and 88.9 per cent of all prosecutions on indictment in the Supreme Court, District Court and Childrens Court of Queensland resulted in conviction65.

By its core function, that being the prosecution of matters in Queensland courts, the ODPP is responsive to the demands placed upon it by the criminal justice system.

Unlike prosecuting authorities in the United States, the ODPP does not generally involve itself in the investigation phase of a matter prior to an offender being charged with criminal offences. If special circumstances exist, there may be some discussions between the ODPP and the QPS, however, this would be a rare occurrence.

Resources

On the issue of adequacy of resourcing, the Acting Director of Public Prosecutions referred to the review of the resourcing of the ODPP by Mr Brian Stewart in June 2013. Mr Stewart’s view was that the ODPP was adequately resourced at that time. The Acting Director of Public Prosecutions clearly stated to the Commission that he had no complaint about resourcing, however, he referred to an increase, since the Stewart review, in the number of charged offences being received by the ODPP and also in the number of indictments presented to the courts.

The Acting Director of Public Prosecutions referred to the fact that the increased workload is but one part of the whole picture. He observes that there has been a change in the way criminal investigations are conducted
and prosecutions litigated, which results in these matters being substantially more resource-intensive. There has been an increase in the size and complexity of the briefs of evidence which requires longer preparation time for trial. Although no statistics are kept by the Office of the Director of Public Prosecutions as to the length of trials conducted, it is perceived that there has been an increase in trial length. Complex investigations that involve protracted and multi-faceted investigations are likely to occur in the investigation of organised crime.

The Acting Director of Public Prosecutions stated that any additional increase in workload brought about by the creation of new offences, an increased rate of charging existing criminal offences, an increased rate of trials due to the requirement to impose mandatory sentences, a continued increase in the consumption of resources due to the preparation requirements for large and complex briefs of evidence, or any other reason, would be monitored closely and set out in the annual report for the Minister. As earlier indicated, the ODPP has a role to play in the administration of Chapter 3 of the Criminal Proceeds Confiscation Act 2002. The Acting Director of Public Prosecutions has indicated that the administration of this scheme has placed some strain on the ODPP. The confiscation of proceeds of crime regimes in Queensland will be discussed in later in this report.

The provision of briefs of evidence

The Terms of Reference required the Commission to examine the adequacy of current legislation and resources available to law enforcement, criminal intelligence and prosecution agencies in Queensland to prevent and effectively investigate and prosecute organised criminal activity.

As part of the examination of the adequacy of the response by the ODPP and in considering the resources attached to the ODPP, the Commission has considered the current practice that is occurring in many organised crime cases where the brief of evidence is provided to the accused or his or her legal representative in electronic format, rather than in hard copy paper form. The provision of briefs of evidence to the defence in criminal matters is a fundamental element of disclosure. It is this brief which determines the way in which a solicitor and counsel approach the charges which the defendant faces. In serious and organised criminal matters, these briefs of evidence are often extensive comprising large amounts of material including statements, exhibits, telephone intercepts, surveillance, bank records, and various analyses which may have been conducted into a person’s affairs.

A practice has developed over the years of these briefs being provided to the defence in electronic form rather than in hard copy. This would appear to be as a result of the initial brief being provided to the ODPP in that form. The ODPP advised the Commission that in circumstances where the ODPP receive the brief from the QPS in that format, it will then be delivered in that format to defence representatives. If a hard copy of the brief is also received that will also be provided. The Acting Director of Public Prosecutions noted that the ODPP did not have a policy as to whether its legal officers would print hard copies for themselves and advised it was a matter entirely for the legal officer.

The President of the Queensland Law Society advised the Commission that the Society does not support the practice of providing electronic-only briefs of evidence to the defence. Mr Michael Fitzgerald provided a number of reasons for this view including:

- The cost involved in printing out the electronic briefs is prohibitive for the vast majority of defendants and their legal representatives. By way of example he provided a number of cost estimates received by his members for these briefs to be printed and they amounted to $22,759.48, $17,006.57, $13,135.32, $14,867.89 and $4,129.16.
- The electronic briefs as currently supplied are not hyperlinked, meaning that a reference in a witness statement to another item of evidence cannot be accessed easily, often requiring the use of several computers at the same time.
The illicit drug market

The Director of Criminal Law at Legal Aid Queensland advised the Commission that while Legal Aid Queensland recognise the benefits of electronic briefs, the experience of Legal Aid staff is that the negatives outweigh those benefits. He highlighted a number of reasons for this view including the following:

- It is difficult and rare to work only from an electronic brief, meaning that a copy will ordinarily be printed for both solicitor and counsel. This causes a significant investment of time and resources and delays the time it takes to have material delivered to counsel.
- There is no consistent form of electronic brief. Some are more user-friendly than others.
- Taking instructions from clients in custody is more difficult and sometimes impossible with electronic briefs.
- There can be a requirement to have a number of types of software to operate different parts of the brief.

It is apparent and understood that for a legal representative to be able to effectively take instructions from their client, and for a solicitor and counsel to be able to effectively work through the brief of evidence, that it is necessary to have a hard copy brief available. In some cases, it may be necessary to have the brief printed three times, allowing for copies to be provided to the solicitor with carriage of the matter, counsel who is briefed in the matter, and for the client to ensure they are aware of the case against them. In addition to financial implications, there is also the concern that those in custody cannot have proper access to briefs in this format, given the limitations of access to computers and the programs operating on those computers prisoners have access to.

The Commission is of the view that justice must be seen to be done to all parties involved in the criminal justice system, in order to ensure the system is working effectively and in a timely manner. As Callinan J in *RPS v R* stated, ‘Justice must be seen to be done. Otherwise justice will not in fact be done.’

It is apparent that the costs associated with parties printing the briefs of evidence which form the basis upon which they are prosecuted are often extraordinary. It is the Commission’s view that for justice to be done to all parties involved in the criminal justice system and to ensure that large organised crime matters proceed in a timely and effective manner, that there should be a requirement that all briefs of evidence are provided to the defence in hard copy format.

This could be achieved by an amendment to section 590AB of the Criminal Code to require all documents to be provided in non-electronic form, as well as in electronic form if the latter is available.

The current practice imposes extraordinary costs upon an individual, in addition to their own costs of legal representation. Given the resources of the State compared to an individual charged, this is unfair and creates the potential for injustices to occur. The Commission takes no view as to which agency should bear the cost of printing hard copies—the QPS or the ODPP. That is an issue for those agencies and the Queensland Government.

**Recommendation**

3.9 The Commission recommends that the Queensland Government amend section 590AB (Disclosure obligation) of the Criminal Code to require all documents to be provided in non-electronic form, as well as in electronic form if the latter is available.
The illicit drug market

Queensland Organised Crime Commission of Inquiry

(Endnotes)

1 Submission of Crime and Corruption Commission, 22 May 2015, p. 36.
3 Submission of Queensland Police Service, 22 May 2015, p. 16.
4 Submission of Queensland Police Service, 22 May 2015, p. 16.
5 Submission of Queensland Police Service, 22 May 2015, p. 16.
7 QPS State Crime Command Organisational Chart [In Confidence].
8 QPS State Crime Command Organisational Chart [In Confidence].
9 Sunshine Coast Daily, 3 January 2015.
11 Statutory Declaration of Ross Barnett, 21 August 2015, para 6 [In-Confidence].
12 Statutory Declaration of Ross Barnett, 21 August 2015, paras 7, 8 [In-Confidence].
13 Statutory Declaration of Ross Barnett, 21 August 2015, para 9 [In-Confidence].
14 Transcript of Interview, Mark Slater, 1 July 2015, pp. 13.
15 Statutory Declaration of Ross Barnett, 21 August 2015, para 11 [In-Confidence].
16 Statutory Declaration of Ross Barnett, 21 August 2015, para 10 [In-Confidence].
17 Statutory Declaration of Ross Barnett, 18 June 2015, para 6 [In Confidence].
24 Transcript of Interview, Mark Slater, 1 July 2015, p. 10 [In-Confidence].
34 Transcript of Interview, Mark Slater, 1 July 2015, pp. 4–5 [In-Confidence].
35 Transcript of Interview, Mark Slater, 1 July 2015, p. 5 [In-Confidence].
38 Submission of Queensland Police Service, 22 May 2015, p. 22.
3.7 Future trends in organised crime in the illicit drug market

It is widely accepted that organised crime is entrenched in the illicit drug market in Australia. As at June 2015, indicative figures drawn from Queensland Police Service (QPS) intelligence reveal that 7 per cent of identified Queensland organised crime networks are involved in the illicit drug market, making the drug market the most prominent form of organised crime in Queensland. Given the lucrative nature of this illicit market, it is anticipated that this trend will continue.
The drugs methylamphetamine (in the form of ‘ice’) and cannabis are the most prevalent drugs in the Queensland community.

The number of people using ice has increased dramatically in recent years, and according to the statistics highlighted in this report, the number of users is likely to continue to increase. More than 60 per cent of Australia’s highest risk criminal targets are involved in the methylamphetamine trade. Of those identified Queensland organised crime networks involved in the illicit drug market, indicative figures as at June 2015, drawn from QPS intelligence, reveal that 51 per cent are linked to the methylamphetamine market.

The ‘ice epidemic’ is not confined to Queensland, evidenced by the formation of the National Ice Taskforce. Users of ice are particularly vulnerable to developing dependency on the drug. One of the most commonly reported side effects of methylamphetamine use is an increased propensity for aggression and violence and the drug has been linked to numerous fatalities. The devastating effects on individuals and their families, the significant health care impacts, and the prevalence of the drug, leads the Commission to view methylamphetamine and in particular, ice, as posing a great risk of harm to Queensland.

Cannabis remains the most commonly used drug in Queensland and Australia. Crop and hydroponic seizures continue to increase. Of those identified Queensland Organised Crime networks involved in the illicit drug market, indicative figures as at June 2015, drawn from QPS intelligence, reveal that 30 per cent are linked to the cannabis market. Due to the high demand and profitability, the market attracts a diverse range of organised crime participants. Family networks and generational operations are particularly dominant in the Queensland cannabis market. It is predicted that these types of organised crime groups will continue to produce cannabis, both hydroponically and in bush form, in Queensland.

While some in the community may view cannabis as a less serious drug, its heavy use is associated with a number of adverse health consequences which ultimately cost the economy and community. Given the prevalence of cannabis use within Queensland and the degree of harm associated with such use, the drug poses a significant risk of harm to Queensland.

Given the increasing prevalence of hydroponic cannabis in Queensland, the Commission has considered the validity of regulating the sale of hydroponic equipment in Queensland. The Commission recommends that the Queensland Government consider amending the Drugs Misuse Act 1986 and Drugs Misuse Regulation 1987 to extend the current end user declaration scheme to hydroponic equipment.

Cocaine, heroin, and MDMA/‘ecstasy’ represent a stable market. There is no indication that Queensland can expect a resurgence in the market of any of these three drugs in the near future; however, their presence in Queensland still calls for appropriate monitoring and policing. MDMA/‘ecstasy’ does, however, remain a very popular drug in Queensland, and if the drug and its precursors increase in availability, it will be an area likely to be targeted by organised crime groups.

Drug analogues and new psychoactive substances have increased in popularity along with the use of the Internet to procure the substances. The ability to change the molecular makeup of different drugs in an attempt to create ‘legal highs’ is fuelling this market. The Commission is of the view that such synthetic substances will continue to increase in popularity as more and more substances flood the market, mimicking the effects of specifically prohibited dangerous drugs. Given the very serious consequences associated with the use of some of these drugs, it is an area of significant risk to Queensland.

The Commission accepts the advice of the Crime and Corruption Commission and the QPS that organised crime groups and in particular, outlaw motorcycle gangs are ready and willing to use violence and extortion to achieve their criminal activities. The Commission also accepts that the use of violence and extortion as an enabler for organised crime and the illicit drug trade will be a continuing issue.

However, the information provided to the Commission and to which the Commission could have regard under its Terms of Reference that might evidence a link between organised crime and violence and extortion was very limited. The Commission received arrest statistics for Operation Resolute from the Queensland Police Service which were of limited assistance. The statistics revealed that a number of outlaw motorcycle gang members were arrested and charged with offences of violence, however the statistics themselves do not show whether the violent conduct was in anyway related to the person’s membership of an outlaw motorcycle gang.
Whenever organised crime groups continue to try and grow their enterprise, violence and extortion will inevitably play a role. It is important that law enforcement agencies maintain a holistic approach to organised crime in Queensland.

Pharmacists are heavily regulated, particularly with regard the dispensing of pseudoephedrine. However, despite such regulation, pharmacists are uniquely placed to enable (knowingly or unwittingly) the production of illicit drugs, through the supply of precursor drugs.

Pseudoephedrine is the most commonly used ingredient in the production of methylamphetamine, a drug whose popularity is growing at an alarming rate. The majority of Queensland pharmacists voluntarily use Project STOP, an online tool which tracks pseudoephedrine sales in real time, and which has had a significant impact on the ability of criminals to source the precursor drug from pharmacies. Given the minimal costs associated with using Project STOP, the Commission recommends that the use of this program by those authorised to dispense pseudoephedrine should be mandatory.

Given the seriousness associated with the drugs detailed in this report, it is vital that Queensland’s dangerous drug offences provide significant maximum penalties which will act as a deterrent. The Commission acknowledges the strong penalties provided in the Drugs Misuse Act 1986 but questions the current two-schedule regime. Queensland has a system whereby illicit drugs are classified between two schedules with higher maximum penalties applying to drugs listed in Schedule 1.

It is the Commission’s view that the two-schedule regime raises a risk for inconsistency in the scheduling of substances, injects a complexity into the penalty regime which renders it less transparent, and sends a confusing message to the community that Schedule 2 drugs are less serious or dangerous than Schedule 1 drugs. The fact that anabolic steroids have been upgraded to Schedule 1, yet a substance such as MDPV which has been linked to fatalities, is listed in Schedule 2, is evidence of the potential for community confusion.

The Commission recommends a move to a single schedule regime where the type of drug does not dictate the applicable maximum penalty. It is the Commission’s view that the penalties applicable to the current Schedule 1 drugs should be retained, resulting in an increase in penalties for the offences of producing, supplying, and trafficking in, current Schedule 2 drugs.

The Commission has identified the use of the Internet to purchase and supply drugs as a growing issue. The Internet and in particular, the Darknet, creates a low-risk environment for individuals and organised crime groups to purchase and sell dangerous drugs. The anonymity offered by encryption-based services and supplying via the post provides protection for offenders.

The Commission recommends that the QPS invest further resources into the area of online drug offending. In particular, additional police officers with sufficient training and expertise in cybercrime should be tasked to monitor online activity, both on the Surface Web and the Darknet, with a view to infiltrating the activities of those selling and purchasing illicit drugs over the Internet. Further, the Commission recommends amendments to the Drugs Misuse Act 1986 to add a new circumstance of aggravation to the offences of possessing, supplying and trafficking in, dangerous drugs, where the Internet is used to facilitate the offence (or in the case of possession, to procure the drug).

Drugs are—and will continue in the future to be—an area of significant concern for the Queensland community. It is imperative that action is taken to address the issues raised in the report.

(Endnotes)

1 Statutory Declaration of Ross Barnett, 18 June 2015, para 6 [In-Confidence].
4.1 Introduction

In accordance with its Terms of Reference, the Commission inquired into the nature, extent, and economic and societal impacts of organised crime in Queensland in respect of Internet, electronic or technology-enabled child sex offending (all referred to in the report as ‘online child sex offending’), including the child exploitation material market.

For the purpose of the Commission’s report, it was determined that online child sex offending included any type of sexual offence committed against a child which occurred as a result of the use of the Internet. This type of offending includes sexual offences involving physical contact between the offender and the child, as well as procuring a child to deal with himself or herself in a sexual way at the direction of the offender. The Commission has also had regard to grooming conduct, contact offending that might occur as a consequence of online child sex offending (such as slavery or trafficking offences, as well as commonly understood contact offences such as rape), maintaining a sexual relationship with a child, and indecent dealing.

Offences relating to the child exploitation material market include any offence arising out of an offender dealing with the material in any way, including making, distributing or possessing such material.

While an offender may be only involved in either online child sex offending or offences relating to child exploitation material, it is not uncommon for an offender to be involved in both types of offending. For example, an offender may make contact with a victim over the Internet and, in the course of communication, direct the child to touch himself or herself, or touch other people, in a sexual way. The offender may then record this conduct and upload the images to the Internet. In this scenario, the offender has not only committed sexual offences against a child, but has also made and distributed child exploitation material. The same offender may also have a collection of child exploitation material which has come into his or her possession quite separately from the sexual offences committed against the child.

In another example, an offender may come to police attention through downloading child exploitation material from the Internet. When the offender’s computer or devices are analysed by police, it may be discovered that he or she has recorded himself or herself committing sexual offences against a child.

This type of offending does not fit neatly within traditional concepts of organised crime. Certain types of online child sex offending—and most aspects of the child exploitation material market—do, however, have features consistent with current notions of organised crime that recognise the changing nature
of such crime, largely on account of technology and globalisation. As Europol recently observed in its call for a new definition of organised crime:

The group structures that dominate fictional representations of organised crime are disintegrating and will increasingly give way to an organised crime landscape dominated by loose networks made up of individual criminal entrepreneurs who interact and conduct their business in a shared, and often digital, criminal underworld.1

Online child abuse and the child exploitation material market are not new phenomena. However, like all types of organised criminal offending, this crime type is fast evolving, alongside advances in technology. It is well known that the Internet has increased the range, volume and accessibility of sexually abusive imagery of children, and has provided an environment for the proliferation of child exploitation material and the creation of an expanding market for its consumption.2 The routine use of the Internet in everyday life has provided expanded opportunities for offenders to gain access to children online.

Offenders in this area are becoming more sophisticated and technically adept, and are often early adopters of new technologies. They use available technology to their advantage in order to avoid detection in the pursuit of their paedophilic and other paraphilic interests. The Commission was told of the alarming demand for increasingly depraved material involving the abuse of children. Membership of some highly networked child exploitation material sites requires the production and uploading of new material—on a regular basis—increasing the demand for child victims.

This ‘virtual criminal underworld’ is largely made up of individual ‘criminal entrepreneurs’ who share their knowledge, experience, expertise and, importantly, their vile and abusive product in a ‘crime-as-a-service’ business model:

Criminal actors, both groups and increasingly individual criminal entrepreneurs, will adopt the crime-as-a-service business model, which is facilitated by social networking online with its ability to provide a relatively secure environment to easily and anonymously communicate.3

In its most recent report on organised crime in Australia, the Australian Crime Commission said that:

Australia is not regarded as a major source of children or material for organised child sex offending. In Australia there is not the same nature or scale of involvement of organised crime groups that have child sexual abuse as the sole or major criminal activity and source of profit for the group.

Organised child sex offending in Australia is also unlikely to involve the more extreme aspects of child sexual abuse facilitated by overseas organised crime groups, including the abduction, trafficking and sale of children. In Australia, it is more likely to involve Australian perpetrators sourcing children and material from like-minded individuals based in Australia, or from overseas-based markets run and facilitated by organised crime groups.4

Notwithstanding that, it is clear that online child sex offending (including grooming and so-called ‘sextortion’) and the child exploitation material market involves networks of offenders. It is also without doubt that Queensland children have been—and will continue to be—victims of abuse in that context. Law enforcement personnel in Queensland are rightly frustrated that there is a lack of understanding in the community, and also perhaps by government and other police, about the increasing extent of the problem, which is addressed below.

This chapter details the nature, extent, and economic and societal impacts of online child sex offending and the child exploitation material market through the lens of modern concepts of organised crime. Sections below set out the range of offending conduct with reference to the offences (both State and Federal) that deal with it.

The prevalence—and societal and economic impacts—of the offending are also addressed in as much detail as possible against the background of chronic under-reporting of this type of offending and the limited availability of empirical data. Those limitations lead to the Commission’s recommendation for the Queensland Government’s proposed independent crime statistics body to prioritise collecting data on and
monitoring the prevalence of organised crime, as well as impacts and trends across all relevant crime types—including online child sex offending.

This chapter also deals with the facilitators or enablers of organised crime in this area. Cyber and technology-enabled crime, as well as IT experts and technical security experts, were identified as being particularly relevant.

The legislative framework in Queensland, for the most part, adequately covers the range of offending in the area of online child sex offending, including the child exploitation material market. The Commission did, however, identify a number of areas that might be strengthened by legislative change or through guidelines that might be developed by a new Sentencing Advisory Council or similar body.

The responses of various agencies to the problem of organised crime in this area are detailed in this chapter. The Commission learned that the Queensland Police Service (in particular, Taskforce Argos) is a world leader in policing online child sex offending. It has forged relationships with international counterparts and has developed skill sets vital to tackling this global problem. Importantly, Taskforce Argos prioritises victim identification, and has been successful in removing many children from harm as a result.

The Cerberus Investigation Unit within the Crime and Corruption Commission also performs important work in this area and is available to assist the Police in its investigations.

Additionally, this chapter also deals with future and emerging trends, highlighting the need for law enforcement agencies to maintain vigilance and flexibility in order to keep pace with this fast-evolving and growing area of organised crime, which targets society’s most vulnerable.

(Endnotes)


4.2 Online child sexual offending

4.2.1 Types of offending

Child sex offending covers a range of offending conduct such as child sexual assault (contact offending), procuring and grooming offences via the Internet (non-contact offending), child sex tourism, child prostitution and trafficking.

In Queensland, since as far back as 2000, officers attached to the Queensland Police Service (QPS) Taskforce Argos have been aware of a growing problem involving networked child sex offenders operating in the online environment.\(^1\) Taskforce Argos is a specialised branch of the QPS responsible for the investigation of online child exploitation and abuse, and its impressive work is addressed in more detail in the section titled Responses, below.

Globally, the increasingly sophisticated online environment has resulted in a ‘tidal wave’ of child sexual offending, particularly within the child exploitation material market. The demand to procure children for
the production of new material for the child exploitation material market is seemingly insatiable. Beyond enabling offending for that purpose, the Internet and associated technology has led to a wealth of further opportunities for offenders, as well as to the evolution of other types of sexual offending against children—including grooming (sometimes resulting in contact offending) and ‘sextortion’ (resulting in the distribution, or threat of distribution, of images and videos obtained by, or for the purposes of, extortion or trickery).

Research undertaken by the Commission, together with information provided by the QPS and the Crime and Corruption Commission (CCC), indicates that networks of offenders involved in online child sex offending are currently operating in Queensland. There are also significant numbers of Queensland children caught up in these enterprises.

Laws relevant to online child sex offending committed in Queensland, by Queensland residents (whether the offending occurs in Australia or overseas), and/or against Queensland children are found in the Queensland and Commonwealth Criminal Codes.

The Criminal Code (Qld)

Contact offending

The Criminal Code contains a range of offences that address sexual misconduct against children where physical contact is an element. Although not strictly falling within the crime category of online child sex offending, contact offending is a concomitant evil in the child exploitation material market, and it is sometimes an extension of online offending such as grooming.

The Criminal Code deals with the following offending involving sexual contact with children:

- indecent treatment of children, including a wide range of conduct ranging from inappropriate touching to oral sex²
- rape and sodomy³
- unlawful carnal knowledge, which includes consensual sex with a child under 16 years⁴
- incest⁵
- maintaining an unlawful sexual relationship (more than one sexual act over any period) with a child.⁶

Those offences carry maximum penalties ranging from 14 years to life imprisonment, and some include circumstances of aggravation that elevate the seriousness and available penalty. For example, the maximum penalty for indecent treatment of a child increases from 14 years imprisonment to life imprisonment if the child is under 12 years of age and/or was a lineal descendent of the offender.

Making a child available for sexual abuse by others is dealt with in a raft of provisions dealing with child prostitution.⁷ The provisions also proscribe obtaining prostitution services from a person who is not an adult. Maximum penalties (for offending relating to children) under these provisions range from seven years imprisonment (for obtaining prostitution services from a child), to 20 years imprisonment (for procuring a child or a person with an impairment of the mind to engage in prostitution).

To date, there are few examples of prosecutions under the State child prostitution provisions. The following is one example, however, of parents prostituting their child for commercial gain. It is a disturbing case, involving a combination of contact offending, maintaining a sexual relationship with a child, and online advertising of the prostitution services offered—including publication of explicit photographs of the child. A web designer was involved in setting up the website.
**R v TR and FV; Ex parte A-G (Qld)**

The parents of the complainant child (who was aged 12 to 13 years) pleaded guilty to a raft of sexual offences (62 for the mother and 41 for the father), including maintaining an unlawful sexual relationship, participating in the provision of prostitution by the complainant, procuring the complainant to engage in prostitution, as well as a number of indecent dealing and rape offences.

TR was the child’s mother and FV the father. The child told police she had lost count of the number of men she had been paid to have intercourse with. She engaged in the conduct because her parents told her they had bills to pay.

A head sentence of 13 years imprisonment was imposed on TR (for the prostitution offences) and ten years imprisonment was imposed on FV (for the prostitution offences). TR was sentenced to six years imprisonment for the offence of maintaining a sexual relationship with the child, and FV was sentenced to seven years imprisonment for the same offence. Under the sentence, TR was required to serve four years before being eligible to apply for parole, whereas FV must serve three years.

The Attorney-General appealed the sentences, specifically, the length of the sentences imposed for the two offences of maintaining a sexual relationship with the child (arguing that they should have been the same as for the prostitution offences), as well as the parole orders. A sentence over 10 years imprisonment for maintaining an unlawful sexual relationship would have automatically attracted a Serious Violent Offence (SVO) declaration and required the offenders to serve 80 per cent of the sentence before becoming eligible for parole. The 13-year terms for the prostitution offences could not be the subject of a SVO declaration, because at that time, the offences were not included in the schedule of offences to which the SVO regime applies. (The Commission notes that section 229G, the offence of procuring a child for prostitution, was inserted in the schedule in 2014).

TR carried on a prostitution service from a motel room and later from an address in an industrial estate. Explicit photographs of TR and the complainant child were found on a website attached to the business. The website advertised the services of TR and the complainant, individually or together.

Numerous, sexually explicit photographs of the complainant were found at the family home and in TR’s belongings. The photographs included evidence of the mother committing sex acts on her daughter. FV admitted he had taken photographs that were then published on the website, as well as other photographs that had been found. The website had been set up with the assistance of a web designer to attract business to the prostitution service.

A diary was found which recorded 28 bookings for the complainant in the period 20 February 2004 to 9 July 2004. There was evidence that the complainant had had sexual relations with other men for money. One man (D) had sexual contact with the complainant over a four-month period. TR was present with the complainant when D arrived at all times, and on the first occasion told him, ‘You can do whatever you want’.

It appears that the basis of the offence of maintaining a sexual relationship with the child included each parent’s roles in the repeated procuring of the complainant to engage in indecent acts with men. The mother was also involved in sexual misconduct (also involving the man, D), and the father took photographs.

The Attorney-General’s appeal was successful only with respect to TR. A sentence of nine years imprisonment was imposed for the maintaining offence, and 18 March 2010 was fixed as the date upon which she was eligible to apply for parole.
Non-contact offences — online child sex offending

The cyber environment provides a relatively anonymous platform from which predators can access countless children. Often posing as children, offenders infiltrate online chat rooms, instant messaging services (including in the context of online gaming), and social networking sites in the attempt to engage young people for various deviant purposes.

Tactics aim to disinhibit children and form a rapport that encourages victims to share personal information and ultimately engage in the predator’s sexual fantasy. That engagement might end with sexually explicit dialogue—or the provision of images or videos—or it might escalate to a meeting where the goal is contact offending.

The Queensland Criminal Code creates offences that deal with the use of the Internet to procure a child to engage in sexual acts, and with ‘grooming’ children.

Using the Internet to procure

Section 218A outlines the offence of using the Internet (or other electronic communication) to procure children under the age of 16. It is committed when an offender procures a child to engage in a sexual act, either in Queensland or elsewhere. ‘Procure’ means to knowingly entice or recruit for the purposes of sexual exploitation.

The maximum penalty is 10 years imprisonment. A maximum penalty of 14 years applies if the child was under 12 years, or the offender believed the child was under 12 years; or, the person met, or went to a place with the intention of meeting, the child.

A person engages in a sexual act if the person allows a sexual act to be done to the person’s body, does a sexual act to the person’s own body or the body of another person, or engages in an act of an indecent nature. The act is not limited to sexual intercourse or acts involving physical contact. The offence applies if the ‘child’ is in fact a police officer posing as a child online.

The following case study is an example of escalating offending, from ‘chatting’ online, to procuring the child to perform sexual acts on line, and ultimately, to contact offending.

Case study

R v Brauer

Brauer pleaded guilty to one count of using electronic communication to procure a person under 16 to engage in a sexual act, one count of using electronic communication to expose a person under 16 to indecent matter, one count of distributing child exploitation material, and three counts of possessing child exploitation material.

Officers from Taskforce Argos and the Coomera Child Protection Investigation Unit went to the defendant’s residence at Mudgeeraba on 10 December 2012. The defendant was not at home; police contacted him and requested that he return home. He arrived home and told police he had used an email account to send and receive emails that contained child exploitation material. The defendant provided the password to the account. Police discovered there were no emails in the account and the defendant admitted that, after being contacted by police, he had deleted the emails from the account. Police were able to retrieve the emails from the trash folder of the account.

Between 2 August 2012 and 8 December 2012, the defendant had sent 25 emails on 15 separate occasions to 44 separate email accounts. In total, the defendant had distributed 180 child exploitation material images and 1 movie file. The 180 distributed images contained a core set of 29 different images. The 29 images were classified as 17 images in Category 1, six images in Category 3 and six images in...
Category 4. The movie file was classified as Category 2. The ‘Oliver scale’ categories are discussed later in this chapter.

An analysis of the defendant’s laptop computer showed he had been using Skype to communicate with a 14-year-old girl who lived in Sydney. Information from the child revealed that the defendant first began to communicate with her when she was 13 years old, when they met on an online social networking site aimed at teenagers, called ‘Habbo’. The defendant had initiated chats with her and told her he lived in Queensland. After a few months communicating through Habbo, they communicated using Windows live messenger. At that point, the child told the defendant she was 13 going on 14 years and the chats turned sexually explicit. They used Skype and the webcam to talk, during which the defendant pressured the child into exposing her breasts and vagina on the webcam. The defendant also exposed his penis to her. About a year after they first met online, the defendant travelled to Sydney, met her at her home and they had sex. The defendant was quite forceful. The child did not really want to have sex; she did not know how to tell him this, and she was afraid of rejection. The defendant and the child met two more times but no sexual activity took place.

The three counts of possession of child exploitation material related to the defendant storing child exploitation material on a USB drive, the laptop computer and on his mobile telephone.

The USB drive contained 67 child exploitation material images, with all five categories being located. The majority of images were classified as Category 1 (27 images), Category 2 (19 images) and Category 3 (10 images). There were nine images classified as Category 4 and two images classified as Category 5.

The laptop computer contained five child exploitation material images, with those classified as Category 1 (one image), Category 3 (three images) and Category 4 (one image). These images were also found on the USB drive.

The mobile telephone contained 353 child exploitation material images and one child exploitation material video which were saved into albums. The majority of the images were classified as Category 1 (138 images) and Category 2 (124 images); however, images were found across all six categories.

The defendant was aged 35 years at the time of the offences and had only one minor previous conviction for stealing, for which a fine was imposed.

The defendant was sentenced to two years imprisonment for each offence and a parole eligibility date was set after six months had been served.

Additionally, so-called ‘sextortion’ is a growing concern and a focus for Taskforce Argos. It is an example of online child sex offending by procuring. The term is used to describe conduct whereby an offender obtains images from a child which have a sexual or compromising aspect to them. This is usually achieved by connecting with a child online, engaging him or her in chat, and then asking for images to be sent. The offender might then use the images in his or her possession to obtain more images by threatening the child. Commonly, the child is threatened that the first set of images will be posted online if more images are not forthcoming.

Sextortion offenders may also direct what sexual activity the child must perform in order for the images not to be published. Sometimes, offenders refer to these images as ‘BM’ images, or ‘Black Mail’ images. Black Mail images are often traded online with other offenders. The offender might boast online about his activities or provide other offenders with the victim’s username. The Commission was informed that websites and forums have been set up for people to trade in such images. Children are reluctant to complain about the offender’s conduct, for fear of embarrassment or shame at the predicament he or she is in. This in turn can lead to the child reaching a breaking point, and causing harm to himself or herself.

The case study, in the section titled Offending involving carriage services, (R v Tahira) outlines a serious example of ‘sextortion’ in Queensland.
Grooming

Section 218B of the Criminal Code creates the offence of grooming children under 16. The offence carries a maximum penalty of five years imprisonment. A maximum of 10 years imprisonment applies if the child is under 12 years, or the offender believed the child was under 12 years.

The offence of grooming is committed if an offender engages in any conduct in relation to a child, with intent to facilitate the procurement of the person to engage in a sexual act or to expose a child to any indecent matter. The offending conduct includes online and ‘real world’ grooming, and it is irrelevant whether the conduct was intended to facilitate the procurement, or expose the child in Queensland or elsewhere. The offence also applies to a situation where a police officer poses as a child online.

The following case study is a disturbing example of this type of online offending. The content is graphic and demonstrates the depraved exploitation of a number of children online. As well as grooming and procuring children to perform vile sexual acts, this offender was also found in possession of a collection of child exploitation material. Although a relatively modest collection in size, a large proportion of the images fell into the worst categories, and reflected the offender’s interest in bestiality.

Case study

R v Kight

Kight pleaded guilty to seven counts of grooming children under 16, three counts of using electronic communication to procure a child under 16, one count of possessing child exploitation material and three summary offences of failing to comply with reporting obligations.

The defendant’s de-facto partner had a Facebook account which she once gave the defendant permission to use. She became aware that he used it frequently and confronted him. He told her that he used her account as he was aware that the authorities, including police and parole officers, monitored his social media use (due to the fact that he was a convicted sex offender—see below).

The de facto partner checked her Facebook account and saw numerous chat logs that contained sexual references and by which the defendant had communicated with girls. She printed out some of the logs, gave a copy to a friend and kept a copy for herself. The friend made a complaint to police about the defendant for an unrelated matter, and provided police with her copy of the logs. As a result of this, the defendant’s residence was searched in August 2013.

During the search, police located a computer which contained child exploitation images. In all, 275 such images and seven movies were found. Of these, 256 images were classified as Category 5 (including a child engaged in a sexual act with an octopus), 11 images were classified as Category 1, six images in Category 2 and one each in Categories 3 and 4. Of the seven movies, there were three classified each in Categories 3 and 5, and one classified in Category 6.

The grooming offences related to the defendant’s communication with six girls using his partner’s Skype account. The girls were aged between 12 and 15 years. On each occasion, the defendant told the girls he was aged 16 years. The conversations with the girls were sexually explicit, and included the defendant asking the girls to show themselves to him on camera.

In the case of four girls, he sent a photograph of an erect penis, purporting to be his. In two cases, after the defendant learned the girls had dogs as pets, he asked them to get the dog. One girl refused to do so and the conversation ended. The second girl agreed and the defendant asked her to force the dog to lick her vagina. The girl said she was doing this and also told the defendant she was having sex with the dog. The defendant asked the same girl if she would ‘fuck’ someone on camera for him, such as a brother, sister or neighbour. He asked her to masturbate herself and she told him she would send videos of herself doing this. The child sent him four videos of her masturbating and inserting an object into her vagina.
These videos formed part of the count of possession of child exploitation material. Another child sent him naked photographs of herself.

The defendant was aged 37 to 38 years at the time of offences, and was aged 39 years at the time of sentence. He had an intellectual impairment and past mental health issues. He had previous convictions in Queensland and Western Australia, including sexual offences against children. The defendant was subject to a suspended term of imprisonment imposed in Queensland for indecent treatment offences when he committed the current offences. He had been earlier sentenced to 18 months imprisonment, suspended after 274 days, with an operational period of two years. The period of 274 days had already been served by the defendant, pending sentence. The defendant had already been dealt with for breaching the suspended term of imprisonment as a result of committing the offences of receiving tainted property and giving false or misleading information. The defendant had been sentenced to a period of six months imprisonment with parole granted after he had served two months. He was still subject to the suspended sentence and parole at the time that the new offences were committed. As a result of other court appearances, the operational period of the suspended term had also been extended.

The defendant was sentenced to three years imprisonment for the three counts of using electronic communication to procure a child under 16 offences, two years imprisonment for the remaining indictment counts, and six months imprisonment for the summary offences. The whole of the balance of the suspended term was also ordered to be served. All terms of imprisonment were ordered to be served concurrently. His Honour ordered the following day as the date for which the defendant was eligible for parole. A period of 223 days which had been served on remand, was declared as time already served.

The following two offences relate to recordings made in breach of privacy and exposing people to obscene publications. They apply to child and adult victims.

**Observations or recordings in breach of privacy**

Section 227A of the Criminal Code applies to adult and child targets of observations or visual recordings made in breach of their privacy. The offence attracts a maximum penalty of two years imprisonment. Offending conduct includes a person being recorded without the person’s consent in a private place, or engaging in a private act in circumstances where a reasonable adult would expect to be afforded privacy. Section 228B relates to the distribution of a prohibited visual recording of a person without the other person’s consent, and attracts the same maximum penalty of two years imprisonment.

**Obscene publications and exhibitions**

Section 228 creates the offence of knowingly, and without lawful justification, selling or exposing persons to obscene publications and exhibitions (including books, pictures, objects and performances). The maximum penalty is two years imprisonment, with circumstances of aggravation that apply when the person depicted is, or is represented to be, a child. In the case of a child under 16 years, the maximum penalty increases to five years imprisonment, and for a child under 12 years, to 10 years imprisonment.

The case summarised below is a good example of a more ‘traditional’, lone sex offender whose brazen contact offending was ultimately detected when he used the Internet to upload child exploitation material to a Russian website.

By distributing the child exploitation material obtained during the course of his contact offending, this offender became part of a network of online child sex offenders.
Case study

R v Goodwin

Goodwin transmitted child exploitation material to a Russian website, which ultimately led to him being convicted of 354 offences relating to child exploitation material offences, burglary offences and offences involving sexual acts against children and adults.

Goodwin was sentenced in the District Court on 23 May 2014. He pleaded guilty to 125 counts of recording in breach of privacy (against section 227A Criminal Code) committed between December 2005 and February 2010, as well as in respect of charges of burglary by breaking in the night (x 13), sexual assault (x 6), burglary and stealing (x 3), burglary, making child exploitation material, indecent treatment of a child under 12 (x 2), observation in breach of privacy, distributing child exploitation material, and possessing child exploitation material.

Goodwin was sentenced to eight years imprisonment for each of the offences of burglary by breaking in the night and burglary; four years imprisonment for each of the offences of sexual assault, indecent treatment, making child exploitation material, and distributing child exploitation material; three years imprisonment for the offences of possession of child exploitation material, burglary, and stealing; and, two years imprisonment for each of the offences of recording in breach of privacy and observation in breach of privacy.

All terms were ordered to be served concurrently, and a parole eligibility date was set on 1 June 2015, after serving two years and four months. A period of 598 days was declared as time already served under the sentence.

The Attorney-General appealed on the ground that the sentences were manifestly inadequate. The appeal was successful, but only to remove the parole eligibility date. The head sentence of eight years imprisonment was undisturbed.

The offending occurred over a period of seven years. Goodwin came to the attention of Taskforce Argos after he sent images of an eight year old girl to a Russian website. Police attended his residence in September 2012, and seized a computer and data storage devices. Goodwin provided authority to police to access his email and online accounts. He denied taking indecent photographs of the eight year old child.

Goodwin admitted that there was child exploitation material on his computer and devices. Police discovered a folder on his computer which contained ‘peeping-Tom’-style voyeuristic images and videos of people in their homes who were unaware of the recordings. The folder was organised into subfolders, which had been named by names, roads and suburbs on the north side of Brisbane.

In October 2012, police again searched Goodwin’s residence, and found a purse with cards of one of the complainants of the burglary offences and other stolen items. Goodwin provided authority to police to access his email and online accounts. He denied taking indecent photographs of the eight year old child.

Goodwin admitted that there was child exploitation material on his computer and devices. Police discovered a folder on his computer which contained ‘peeping-Tom’-style voyeuristic images and videos of people in their homes who were unaware of the recordings. The folder was organised into subfolders, which had been named by names, roads and suburbs on the north side of Brisbane.

In October 2012, police again searched Goodwin’s residence, and found a purse with cards of one of the complainants of the burglary offences and other stolen items. Goodwin provided authority to police to access his email and online accounts. He denied taking indecent photographs of the eight year old child.

Goodwin admitted that there was child exploitation material on his computer and devices. Police discovered a folder on his computer which contained ‘peeping-Tom’-style voyeuristic images and videos of people in their homes who were unaware of the recordings. The folder was organised into subfolders, which had been named by names, roads and suburbs on the north side of Brisbane.

In October 2012, police again searched Goodwin’s residence, and found a purse with cards of one of the complainants of the burglary offences and other stolen items. Goodwin provided authority to police to access his email and online accounts. He denied taking indecent photographs of the eight year old child.

Goodwin recorded some footage by peering through windows of the various homes. For that offending, he was charged with recording in breach of privacy. Some of the recordings relate to different complainants within the one household. Goodwin also broke into some houses to make recordings. In respect of that conduct, he was charged with burglary by breaking in the night as well as recording in breach of privacy.

One of the houses was visited 14 times by Goodwin, and two adult women were video-recorded. In one instance, Goodwin was inside the house and recorded one of the women asleep. On another occasion, one of the women reported being poked on the bottom during the night.
Another house was visited by Goodwin 12 times. He entered that house 10 times. Four offences of sexual assault were committed against the daughter (aged 14 to 18 years over the period), which included Goodwin touching her variously on the breasts, buttocks, anus and vagina while recording this activity. On one occasion, the complainant woke to find Goodwin on top of her with his penis in her face. She screamed and her father chased Goodwin outside the house but was unsuccessful in his attempt to catch him. There was a further occasion when the daughter woke to find Goodwin in her bedroom and police were called.

At the same house, a cousin (aged 25 years) was sleeping in the daughter’s room, and 40 videos were taken by Goodwin, during which the camera moves back and forth between the two girls as they slept. On occasions, Goodwin tried to—and was sometimes successful in—moving bedclothes to expose the breast, stomach and pubic areas of the older girl. He also captured himself masturbating whilst he was in the bedroom.

At a different house, the complainant girl (aged eight years) was videoed by Goodwin. He possessed 15 still images taken from the recording which showed him pulling aside her underpants and taking close-up shots of her genital area, buttocks and anus. The indecent treatment counts relate to this conduct as well as some child exploitation material offences. Images of this complainant were uploaded to the Russian website and are the subject of the charge of distributing child exploitation material.

Another set of offences related to the theft of electronic photographs stored on the complainant’s laptop. Goodwin visited this house eight times and recorded the complainant dressing in her bedroom. The mother of this complainant was also recorded on the toilet, in the shower, and dressing.

A male complainant in a separate house was filmed in the bathroom but saw a camera outside the window. He yelled at the person and the camera disappeared. There was one offence of burglary which did not involve a sexual offence or a recording.

Goodwin held an extensive collection of child exploitation material on his hard drives, and this relates to the offence of possessing child exploitation material. The collection included videos and images in each of the five categories, with over 1,100 videos and over 150,000 images being found.

Goodwin was aged 33 to 41 years over the period of offending, and had a minor criminal history. This included dated convictions in New South Wales for entering enclosed lands related to graffiti, and Queensland convictions for stealing from a locked receptacle for which a probation order was imposed. There was evidence before the court of a traumatic and abusive childhood, coupled with a history of depression after being rejected by the army.

The Criminal Code (Cth)
The Commonwealth Criminal Code deals with a wide array of sexual offending against children, including offending by Australian citizens outside Australia.

Slavery and servitude

This type of offending is dealt with under Division 270 of the Criminal Code (Cth). The offences include slavery under section 270.3, servitude under sections 270.4 and 270.5, forced labour under section 270.6 and deceptive recruiting for labour or services under section 270.7.

In respect of servitude, forced labour, and deceptive recruiting, an aggravated offence applies if the victim is under 18 years of age (section 270.8). All offences relate to the exploitation and restriction of people.

The maximum penalty for slavery is 25 years imprisonment and, for being involved in a commercial transaction for a person enslaved, 17 years imprisonment. The maximum penalty for the offence of servitude is 15 years imprisonment, unless it is an aggravated offence, which attracts a maximum penalty of 20 years imprisonment.
The maximum penalty for the offence of forced labour is nine years imprisonment, unless it is an aggravated offence, for which the maximum penalty is 12 years imprisonment. For the offence of deceptive recruiting, the maximum penalty is seven years imprisonment, unless it is an aggravated offence, for which the maximum penalty is nine years imprisonment.

**Trafficking of children**

Division 271 of the Criminal Code (Cth) applies. Child trafficking offences relate to the movement of children both into and out of Australia (under section 271.4), as well as the movement of children from one place to another within Australia (under section 271.7).

The offence of trafficking in children is established where an offender arranges for the movement of a person under the age of 18 years, either with the intention of, or being reckless about, the person being used to provide sexual services or to be otherwise exploited by the offender or by someone else.

The trafficking in children offences attract a maximum penalty of 25 years imprisonment. There is no mirror provision in Queensland, and that potential gap in the state legislation is discussed in Part 4.5 (Legislative gaps) below.

In Australia, human trafficking and slavery matters have mainly involved opportunistic groups of criminals, rather than large, traditionally structured organised crime groups. Since the introduction of Divisions 270 and 271 of the Commonwealth Criminal Code, 16 individuals have been convicted of human trafficking or slavery-related offences. Ten of those individuals were convicted of slavery offences, four of sexual servitude offences, and two of human trafficking offences. The Commission found a small number of cases in Queensland involving offenders dealt with for child trafficking and/or child prostitution offences. None of them appear to be related to online child sex offending, although one case involved the publication of explicit photographs of a child victim for advertising purposes (see Case study: R v TR & FV; Ex parte A-G above). The case of R v KAK (below) is the only Queensland case that the Commission was able to identify that involved the Commonwealth offence of trafficking in children.

**Case study**

*R v KAK*\(^{15}\)

**The Operation**

In 2011, Operation Juliet Ostrich was conducted by the QPS into sexual offences committed against a young girl by her mother (KAK), a masseuse-turned-prostitute, in Runcorn on Brisbane’s Southside. As a result of the operation, the child’s mother and some of her clients were charged in respect of their offending against the child.

**KAK**

KAK pleaded guilty to trafficking in children and procuring prostitution of a young person under the Criminal Code (Cth), as well as multiple counts of indecent treatment of a child under 12 who was a lineal descendant, indecent treatment of a child under 16 who was a lineal descendant, and maintaining an unlawful sexual relationship under Criminal Code (Qld). Of all the offending conduct, the State offence of maintaining an unlawful sexual relationship attracted the highest maximum penalty—life imprisonment.

By her plea of guilty to trafficking in children, KAK admitted she had arranged for her daughter to come to Australia to live with the intention that she be used for sexual exploitation. Thereafter, KAK engaged in a graduated process involving systematic behaviour, requiring her daughter (from the age of nine) to engage in prostitution.
A sentence of nine years imprisonment was imposed for the trafficking and prostitution offences; seven years imprisonment was imposed for the maintaining offences, and three years imprisonment was imposed for the indecent treatment offences. A non-parole period/parole eligibility date was set at four years.

The defendant appealed the sentences imposed with respect to the trafficking and prostitution offences, together with the parole orders imposed, and was successful in having the nine-year terms imposed for the trafficking and prostitution reduced to seven years imprisonment, as well as a non-parole period/parole eligibility set at three years and six months.

Muir JA commented that if KAK’s conduct was recognisably outside the worst category of cases for which the 14 year penalty for procuring was prescribed, it was only marginally so. Further, it was said that:

"[T]he offending conduct, involving as it did the substantial corruption and degradation of the applicant’s daughter from an early age for monetary gain, was singularly abhorrent and merits strong denunciation."

It was KAK’s significant cooperation with law enforcement that warranted the reduction in her sentence.

**KAK’s Clients:**

**R v Baxter:** Baxter pleaded guilty to 13 sexual offences including indecent dealing with a child under 12, maintaining an unlawful sexual relationship and a number of counts of obtaining prostitution from a person who is not an adult. KAK introduced the complainant into the sexual activities that occurred between herself and Baxter. This commenced when the child was aged nine years, and continued for a number of years until January 2011. The offending ceased when the child ran away from home and told friends what had occurred. Baxter was sentenced to seven years imprisonment with respect to the maintaining offence, four years imprisonment with respect to the prostitution offences and two and a half years imprisonment with respect to the indecent dealing offences. A parole eligibility date was set after two years and four months was served.

**R v Sirianni:** Sirianni was a client of KAK and pleaded guilty to one count of obtaining prostitution from a person who was not an adult (KAK’s daughter). He was sentenced on the basis that he was involved on one occasion with the complainant; that he expected the sexual act to be conducted by KAK and thought the complainant was the sister of KAK, not her daughter. He was fined $1,500 and a conviction was not recorded.

---

**Offending involving carriage services**

Offences were introduced in 2004 to prohibit the use of a carriage service (telephone, Internet, email and other applications) for sexual activity with a child, as well as for child abuse and pornography material. This section of the Commission’s report outlines the offences relevant to online child sex offending. The use of carriage services in the child exploitation market is dealt with below in the section titled Online child exploitation material market.

Section 474.25A creates the offence of using a carriage service for sexual activity with a child under 16 years, and attracts a maximum penalty of 15 years imprisonment. A maximum of 25 years imprisonment applies if the child has a mental impairment, or the offender occupies a position of trust or authority with respect to the child, or the child is under that person’s care, supervision of authority, pursuant to section 474.25B.

Section 474.26 creates the offence of using a carriage service to procure a child under 16 years to engage in sexual activity, and attracts a maximum penalty of 15 years. The offence of using a carriage service to groom a child under 16 years is set out in section 474.27. The maximum penalty is 12 years imprisonment. Section 474.27A deals with offending involving the use of a carriage service to transmit indecent communication to a child under 16 years. The maximum penalty is seven years.
Case study

R v Tahiraj\(^\text{18}\)

Tahiraj held two internet accounts. Using the profile name ‘Tick Tock’, he met a 13-year-old girl via the website www.vampirefreaks.com. She told him she was 13, turning 14. Tahiraj told her that he was good at hacking and he could get her more friends on MySpace. She added his email address on MSN Messenger. He sent her a program over MSN Messenger, which she downloaded onto her computer.

Using this program, Tahiraj was able to access and turn on her webcam remotely. The pair spoke the next day via MSN Messenger, and she asked Tahiraj about obtaining more friends on MySpace. He turned on her webcam remotely and when she tried to block him on MSN Messenger, he made a countdown appear on her screen and threatened to destroy her computer if she did not unblock him.

The girl complied, and Tahiraj told her to strip on webcam. He threatened to destroy her computer and hack her online accounts if she did not. Tahiraj instructed her to masturbate on webcam and write something on her breasts. This was recorded by Tahiraj, and he then uploaded the recording to the Internet via the website ‘Rapidshare’.

As a result, several people on VampireFreaks and MySpace tried to message the complainant and add her as a friend. She was very distressed by the incident, but did not tell anyone about it. Later, she deleted her email account.

During March and April 2009, Tahiraj made contact, using the same Internet account, with a 14-year-old girl, whom he also met through the website VampireFreaks. This complainant added Tahiraj onto her MSN Messenger account. Via VampireFreaks, Tahiraj told her he wanted to see more of her. He said, ‘Fuck me’ and ‘do you want to meet up for sex?’ She declined, and he called her ‘dumb’, ‘stupid bitch’ and ‘slut’. She blocked him, but he created another VampireFreaks account and repeated his actions, asking her to meet up for sex. He sent her files on MSN Messenger which she did not open.

From November 2008 to April 2009, an officer attached to the cybercrime team of the Australian Federal Police (AFP) monitored the website ‘unkn0wn.ws’. He saw a message posted by the user ‘Rofles’ which said,

I’m Rofles, I destroy lives....I make a girl cry. I force her to strip and fuck herself. I force her to finger her asshole and lick her fingers. I then make her write a greetz to a mate of mine on her tits. Epic win?

This message was connected to the video of the 13 year old girl, which had been posted by Tahiraj. The IP address of Tahiraj was the one which posted the video.

On 8 April 2009, officers with the AFP went to Tahiraj’s address at Northlakes, and seized his computer and hard drives. An analysis of the items revealed that Tahiraj had accessed child exploitation material (124 images, 1 video and 7 partial videos) and child abuse material (6 images) using his Internet account. In addition, 64 images of child exploitation material were found stored on the computer and a hard drive. Images and videos belonging to each of the five categories in the Oliver scale were found.

A computer hacking program called ‘Poison Ivy’ was found on the seized computer. An analysis showed that he had used the ‘Poison Ivy’ program to hack into the 13-year-old complainant’s computer and 133 others. The 13-year-old complainant’s computer was configured so that the ‘Poison Ivy’ program would start automatically when the computer was turned on.

Tahiraj was aged 19 years at the time of the offending and 24 years at the time of sentence. He had no previous convictions.

Tahiraj was charged with two counts of using a carriage service to procure a person under 16 years, unauthorised access to a computer with intent, using a carriage service to make child pornography
material available, using a carriage service to access child pornography material, using a carriage service to access child abuse material, and possessing child exploitation material.

After a trial at which he was convicted, Tahiraj was initially sentenced to an effective term of 12 years imprisonment, as a result of a series of cumulative terms being imposed. A non-parole period of six years imprisonment was set, and a period of 71 days was declared as time already served. As a result of a successful appeal against sentence, an effective term of eight years imprisonment was imposed, with a non-parole period of four years.

Child sexual offending outside Australia

Division 272 of the Criminal Code (Cth) provides for the prosecution of Australian citizens and residents who commit sexual offences against children outside Australia. The offences relate to contact offences against children, as well as procuring or grooming a child to engage in sexual activity.

Division 272 was introduced in 2010 with the enactment of the Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010 (Cth). That Act included a raft of amendments relating to sexual offences against children. The Explanatory Memorandum to the Bill explained that:

‘[t]he amendments will ensure comprehensive coverage of sexual offences against children within Commonwealth responsibility, including reflecting best practice approaches domestically and internationally.’

The provisions aim to strengthen existing laws relating to child sex tourism, and created new offences including an aggravated offence, a persistent sexual abuse offence, and offences of procuring and grooming children outside Australia.

Procuring and grooming (by making it easier to procure) children under 16 years to engage in sexual activity outside Australia attracts maximum penalties of 15 and 12 years respectively.

The case study below provides an example of the kind of online child sexual offending captured by these provisions. The conduct involves a transnational network of child sex offenders.

Case study

*Rivo v R*[^20]

Upon the execution of several search warrants, AFP officers seized evidence showing that Rivo had procured live sex shows involving children as young as eight years old. Analysis revealed chat sessions with people in the Philippines who outlined the cost involved ($35 to $60 for live sex shows) and payment method (via alternative remittance provider Western Union).  

During numerous separate sessions, Rivo acted as ‘film director’, providing instructions to the procurers and to the children performing sex shows live. The instructions he gave, described in detail in the judgement, are vile and demeaning, and no doubt contributed to significant harm to the children involved. Those children were almost certainly made available to many more like Rivo.

Photographs were offered to Rivo, including depictions of bestiality involving children. He offered to pay double for such images.

The live sex shows were not recorded; however, sufficient information remained in the chat logs to show details of their nature.

In the final chat session, Rivo indicated that he wanted to have sex with a child, and indicated his intention to travel to the Philippines in the near future.
The sentencing judge made the following comments:

While you did not physically abuse these children yourself, the line between your conduct in directing the actual sexual activities carried out on and by the children for your sexual gratification is so thin as to be virtually non-existent. To put it plainly, you called the shots, you decided what was to be done to and by these children. You were directly responsible for the contents of the sex shows. On behalf of this community, I denounce your conduct and I sentence you as follows...

Six years imprisonment was imposed for procuring children to engage in sexual acts outside Australia, and four years imprisonment for causing child pornography to be transmitted to himself. The non-parole period was set at five years. Had it not been for Rivo’s plea of guilty, the judge would have imposed a head sentence of 10 years imprisonment.

Contact offending by Australians against children outside Australia is dealt with in sections 272.8–272.13 of Division 272. The provisions differentiate between sexual intercourse and sexual activity, and provide different maximum penalties depending on whether the victim is under 16 years (a child), or over 16 years but under 18 years (a young person).

A person who causes a child to engage in sexual intercourse in the presence of that person is liable to prosecution under these provisions.

Aggravated offences apply if the child or young person suffers a mental impairment or is under the care, supervision or authority of the offender. In that case, for sexual intercourse with a child, the maximum penalty is 25 years imprisonment.

Persistent sexual abuse of children (on three or more occasions) also attracts a maximum penalty of 25 years imprisonment.

4.2.2 Prevalence of the offending

It is difficult to capture a true picture of the prevalence of sex offending against children in Queensland and/or by Queenslanders. Estimates vary considerably for a range of reasons, including the method of data collection and variations in definitions used.21

Further, and significantly, it is well known that child sex offending is under-reported. Reasons for the under-reporting of child sex offences are varied and include:

- the vulnerability of the victims
- the young ages of the victims
- the inaccessibility of trusted figures to whom victims can complain (particularly in circumstances where the offender is the person whose role it is to protect the victim)
- the stigma attached to this type of offending
- an inability to recognise the reality of what is happening
- emotional and other social factors.

Given the difficulties in ascertaining the prevalence of sex offending against children generally, it is impossible to provide a true indication of the extent of online child sex offending insofar as the organised crime landscape in Queensland is concerned. It is possible to say however, that those working to combat crime in this area describe a constantly evolving global problem to which Queensland is not immune.
**Facts and figures**

The research undertaken by the Commission found a variety of statistics which record information relating to the sexual abuse of children. The information captures different aspects of the reporting of child abuse cases by government entities, the reporting of sexual abuse cases to the QPS, the prosecution of offenders in Queensland courts, and the results of surveys conducted by the Australian Bureau of Statistics. In each case, the statistics generated have limitations and caveats placed on them by the recording body.

It became evident to the Commission that the lack of helpful statistical data applies across all crime types comprising the key areas of focus under the Terms of Reference (the illicit drug trade, online child sex offending—including the child exploitation material market—and financial crime) such that the Commission considers that there is a need for an independent body to fulfill a research and statistical analysis role in respect of criminal offending in Queensland, in particular to improve the understanding of the prevalence of organised crime across the state.

The Queensland Government has stated its commitment to establishing such a body, which will 'publish independent crime statistics for all criminal offending across Queensland.' The Commission was unable to establish the progress of that commitment, but supports its delivery.

A range of results are set out below to demonstrate the lacuna in statistical data and analysis that might assist the Queensland Government, law enforcement, and prosecution agencies to assess priorities—including resource allocation—in the context of addressing organised crime (in this case in the area on online child sex offending) in Queensland.

**Australian Institute of Family Studies (Australian Government)**

The Australian Institute of Family Studies published a resource sheet in July 2015 which sets out statistics regarding child abuse and neglect across the country. The information was drawn from the report by the Australian Institute of Health and Welfare entitled ‘Child Protection Australia 2013–2014’.

Since 1990, the Australian Institute of Health and Welfare has compiled annual national figures for child protection activity. The statistics relate to data that includes instances of notification, investigation and substantiation of allegations, care and protection orders, and out-of-home care figures.

Historically, different definitions of what constitutes child abuse and neglect across the states and territories has made it difficult to obtain consistent and comparable national statistics. However, in recent years there has been a move to develop a structured data set that will enhance the reliability of information collected across the country, benefitting national reporting and research.

Despite that, jurisdictional variations remain in areas such as mandatory reporting, notifications and substantiation thresholds, so that 'when interpreting the national figures, different legislation, policies and procedures of each state and territory should still be taken into account.' As the research sheet states, 'it is also important to consider that not all children identified in these statistics will necessarily have been maltreated. Child protection authorities are required to intervene if a child has been, is currently being, or is at risk of being, harmed. Therefore a certain proportion of children in these statistics will be those who have not been harmed, but are at risk of future harm.'

'Notifications' consist of allegations of child abuse (physical and sexual) or neglect, child maltreatment or harm to a child made to an authorised department. 'Investigations' are the process by which departmental staff obtain more information about the child the subject of the notification and an assessment is made about the harm and the child's protective needs. 'Substantiations' of notifications occur when an investigation is complete and there is reasonable cause to believe that the child had been, was being, or was likely to be abused, neglected or otherwise harmed.

For the 2013–2014 period, across all states and territories, there were a total of 40,571 children who were the subjects of substantiations of notifications. This figure represents substantiations of all types of abuse, which
include emotional abuse, neglect, physical abuse and sexual abuse. The results, by state and territory, are set out below:\(^{27}\)

### Primary substantiated harm types in Australian states and territories, 2013–2014

<table>
<thead>
<tr>
<th>Harm type</th>
<th>NSW</th>
<th>VIC</th>
<th>QLD</th>
<th>WA</th>
<th>SA(^a)</th>
<th>TAS(^a)</th>
<th>ACT(^b)</th>
<th>NT(^b)</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emotional abuse</td>
<td>4,767</td>
<td>6,453</td>
<td>2,420</td>
<td>1,003</td>
<td>601</td>
<td>315</td>
<td>97</td>
<td>437</td>
<td>16,093</td>
</tr>
<tr>
<td>Neglect</td>
<td>4,740</td>
<td>572</td>
<td>2,883</td>
<td>967</td>
<td>1,013</td>
<td>212</td>
<td>142</td>
<td>665</td>
<td>11,194</td>
</tr>
<tr>
<td>Physical abuse</td>
<td>2,686</td>
<td>2,927</td>
<td>1,040</td>
<td>480</td>
<td>367</td>
<td>114</td>
<td>33</td>
<td>259</td>
<td>7,906</td>
</tr>
<tr>
<td>Sexual abuse</td>
<td>2,881</td>
<td>1,443</td>
<td>342</td>
<td>603</td>
<td>208</td>
<td>57</td>
<td>14</td>
<td>33</td>
<td>5,581</td>
</tr>
<tr>
<td>Total</td>
<td>15,074</td>
<td>11,395</td>
<td>6,685</td>
<td>3,053</td>
<td>2,109</td>
<td>712</td>
<td>1,394</td>
<td>1,394</td>
<td>40,844</td>
</tr>
</tbody>
</table>

Notes:

\(^a\) In South Australia, Tasmania, and the Australian Capital Territory, the abuse type for some of the substantiations was recorded as ‘not stated’ (70 cases) and could not be mapped to physical, sexual, emotional abuse or neglect. These substantiations are included in the totals; as such, totals may not equal the sum of categories.

\(^b\) In the Northern Territory, due to recording issues, sexual abuse is under-reported. This has been addressed and it is expected that numbers in this area will be similar to other jurisdictions in future years.

Source: AIHW (2015, p. 73)

There are a number of limitations on the use of this data. The obvious limitation for understanding the nature and extent of organised crime in the area of child sex offending is that the data is restricted to reported conduct within family units.

Even within those parameters, the resource sheet details further limitations, including:

- The child protection statistics only collect data about those children who come into contact with child protection services. The data excludes cases where the abuse or neglect was not caused by the parent, but by a non-family member.
- Some children who have not been abused or neglected have been included in the statistics: for example, a child who needs care and protection as a result of a parent being hospitalised with no other family member able to care for the child; or, a child at risk of being abused but who has not yet experienced abuse—for example, a child whose step-parent is a convicted child sex offender.
- Child protection data have been perceived as a conservative estimate of the incidents of child maltreatment.
- Child abuse and neglect often go undetected due to the private nature of the crime, the difficulties children experience in making disclosures, and the lack of evidence to substantiate the crime. Therefore, the statistics only record those cases of abuse and neglect that are detected and reported.
• Child protection data reflect only those families reported to child protection services. Economically disadvantaged families are more likely to come into contact with, and therefore under the scrutiny of, public authorities. This means that it is more likely that abuse and neglect will be identified in economically disadvantaged families if it is present.


This statistical data collection collates information from across Australia in respect of many facets of victims of crime. The offence types included homicide and related offences, sexual assault, kidnapping/abduction, robbery, and blackmail/extortion. The data records matters that come to the attention of—and were recorded by—police between 1 January 2014 and 31 December 2014. The information was taken from administrative systems maintained by state and territory police services.

One table in the collection recorded victims by age, sex and state or territory. With respect to the offence of sexual assault in Queensland and relevant to children, the following information was recorded:

<table>
<thead>
<tr>
<th>Age group (years)</th>
<th>Males</th>
<th>Females</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–9</td>
<td>237</td>
<td>409</td>
</tr>
<tr>
<td>10–14</td>
<td>185</td>
<td>941</td>
</tr>
<tr>
<td>15–19</td>
<td>134</td>
<td>871</td>
</tr>
<tr>
<td>Total</td>
<td>556</td>
<td>2,221</td>
</tr>
</tbody>
</table>

**Personal Safety, Australia, 2012, Australian Bureau of Statistics**

This statistical data collection collated information from a national survey conducted from February to December 2012, with the findings released in December 2013. The survey was not compulsory, and 13,307 women and 3,743 men completed it. The survey collected information from men and women about the nature and extent of violence experienced since the age of 15. It also collected information about the participants’ experience of current and previous partner violence, lifetime experience of stalking, physical and sexual abuse before the age of 15, as well as sexual harassment and feelings of general safety.

A weighting process was used in this survey. This is the process of adjusting results from a sample survey to infer results for the total in-scope population. The in-scope population for this survey was people aged 18 years and over, living in private dwellings across Australia.

Data was collected about participants’ experience of physical or sexual abuse by an adult before the age of 15 years. ‘Abuse before the age of 15’ was defined as sexual or physical abuse experienced by a person before the age of 15 years from any adult, male or female, including the person’s parents.

One table in the collection sets out the survey results relating to the experience of the participants of physical and/or sexual abuse before the age of 15 years. The results do not distinguish between physical and sexual abuse, nor are they broken down into states or territories.

After the weighting process was undertaken, the results indicated that the total number of males in the Australian population (approximately 23 million) who had experienced abuse before the age of 15 years was 1,067,700. The total number of females was 1,668,400.

The survey is cited as concluding that 12 per cent of women and 4.5 per cent of men reported having been sexually abused before the age of 15 years. That figure, of course, says nothing about the precise nature of the sexual offending, or whether there was any element of networked offending.

The collection includes information on the offences, case outcomes, and sentences imposed in each state and territory criminal jurisdictions relating to the Higher (Supreme and Intermediate), Magistrates’ and Children’s Courts. The information is derived from data provided to the Australian Bureau of Statistics by the state and territory agencies responsible for courts administration. In Queensland, data was supplied through the Office of the Government Statistician.

The data collection also collates information relating to Queensland Courts. The information is collated according to the principal offence, and there are a number of offence categories used. For child sex offences, the relevant category is ‘Sexual assault and related offences’. This category includes sexual assault, aggravated sexual assault, non-aggravated sexual assault, non-assaultive sexual offences against a child, child pornography offences, sexual servitude and non-assaultive sexual offences.

The major limitation of this data collection, for the purpose of understanding the nature and extent of child sex offending, is that the only relevant category does not distinguish between sexual offences committed against adults, compared with those committed against children. The data available within this collection does not, therefore, assist in determining the number of defendants dealt with for sexual offences committed against children, or for computer-related child sexual offences.

The Annual Report sets out statistics that relate to ‘Crime and Public Order’. It reports the rate of personal safety offences reported per 100,000 people. Under the category of ‘Sexual assault’, 110 offences per 100,000 people were reported.

Relevantly, it was further reported that, from 1 July 2013 to 30 June 2014, Taskforce Argos detectives:

- rescued 159 children nationally and internationally
- finalised three international operations
- referred 331 targets to partner law enforcement agencies, both nationally and internationally
- prosecuted 145 offenders on 596 charges
- reviewed over 206,467 seized child exploitation images and 624 hours of child exploitation video.

There are no other reported statistics that relate to child sex offences available in the QPS Annual Report.

During the course of the Inquiry, further statistics were obtained from the QPS in respect of other operations conducted by Taskforce Argos. In respect of Operation Rhodes, from 1 July 2014 to 30 June 2015, detectives from that unit:

- finalised a major international operation seizing administrator control of a large child exploitation network, leading to the arrest of a South Australian child protection worker for contact sexual offences against seven children (see Case study: Shannon McCooie)
- referred 180 targets to partner law enforcement agencies, both nationally and internationally
- rescued 68 children from harm
- charged offenders with making and distributing child exploitation material and contact offences against children (including rape and sexual assault).
The Commission was also informed that Operation Commitment, established in July 2012, has achieved the following results:

- 195 premises searched, locating child exploitation material in 193 premises (98.97% of premises searched)
- of the premises searched, 123 people were confirmed to be contact offenders (63.08%) and 191 victims were identified
- 239 further suspects were identified as a result of the initial search of 195 premises. Of those 239 suspects, 207 (86.6%) were found with child exploitation material, 30 (12.5%) were confirmed to be contact offenders and a further 52 victims were identified.

**Crime and Corruption Commission**

Detective Senior Sergeant Cameron Burke, the Operations Leader of the Cerberus Unit at the CCC, informed this Commission that 193 alleged online child sex offenders were arrested from 2004 until 22 July 2015. Those arrested have been charged with 2,825 offences, and 344 of those charges were laid against Queensland residents. In addition, as a result of the operations conducted by the Cerberus unit within the same period, there have been 35 referrals to other Queensland law enforcement agencies or associated organisations, 111 interstate disseminations, and 106 international disseminations. A dissemination occurs when information concerning alleged offences is passed onto the relevant law enforcement agency of another jurisdiction for investigation and/or action.


The Annual Report sets out statistics that relate to offences received for prosecution from 1 July 2013 to 30 June 2014. Statistics relating to offences under the headings of homicide, sexual, violence, drugs, property, motor vehicle, other offences and breaches are outlined. With respect to sexual offences, the offence types include adult, maintaining sexual relationship, child and computer related. Across the state, the following totals are listed:

- adult (adult complainant): 727
- maintaining sexual relationship: 49
- child (child complainant): 4,046
- computer related: 1,712

Again, the statistics do not isolate sexual offending with an element of networking or organisation such as to assist the Commission in its task, or other agencies in responding to or assessing risk in respect of organised crime in this area.

**Commonwealth Director of Public Prosecutions — Annual Report 2013–2014**

The Commonwealth Director of Public Prosecutions Annual Report sets out statistics for charges dealt with in the period from 1 July 2013 to 30 June 2014. These statistics are not broken down by state or territory, and therefore reflect prosecutions across the country. That is an obvious limitation for present purposes.

Notwithstanding that, statistics are provided for each of the relevant Commonwealth offences in the area of online child sex offending, with reference to the sections of the various pieces of legislation that come under the realm of Commonwealth prosecutions. The statistics are further separated, depending on whether the offences were dealt with summarily (in the lower courts) or on indictment (in the higher courts). The relevant statistics are as follows:
### Section and Offence (Criminal Code)

<table>
<thead>
<tr>
<th>Section and Offence</th>
<th>Summary</th>
<th>Indictable</th>
</tr>
</thead>
<tbody>
<tr>
<td>272.14(1)</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>272.15(1)</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>273.5(1)(a)(i)</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>273.5(1)(a)(ii)</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>474.19(1)</td>
<td>0</td>
<td>241</td>
</tr>
<tr>
<td>474.20(1)(a)(i)</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>474.22(1)(a)(i)</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>474.22(1)(a)(iii)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>474.24A(1)</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>474.25A(1)</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>474.26(1)</td>
<td>0</td>
<td>43</td>
</tr>
<tr>
<td>474.26(2)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>474.27(1)</td>
<td>0</td>
<td>39</td>
</tr>
<tr>
<td>474.27A(1)</td>
<td>14</td>
<td>58</td>
</tr>
</tbody>
</table>

### Department of Justice and Attorney-General

The Commission sought information from Mr David Mackie, Director General of the Department of Justice and Attorney-General (DJAG), regarding the collation and retention of statistics of court outcomes in Queensland.

The Commission was advised that certain data is kept about offenders convicted in the Magistrates, District and Supreme Courts. That database included the name, date of birth, gender, single person identifier number, indigenous status, occupation, language spoken, driver license number, place and country of birth, telephone...
number, email address and any alias used. Past criminal records are not captured in the database, and there are no links between files for the same offender.

Stored details regarding convictions include:

- the type of offence, including the statute, section number and any circumstance of aggravation
- the date of all court events
- the outcome of each charge at each court event
- the judicial officer
- the court type and location
- the orders imposed for each charge.

This information is sourced from the Queensland-Wide Interlinked Courts (QWIC) database, and the Commission was advised of some limitations of the statistics. For example, some of the database fields are not mandatory, and are referred to as ‘free text.’ An example of free text fields are the place and country of birth, occupation, driver licence number, language, telephone number, email address and alias. Those fields are not suitable for statistical analysis.

Further, there are limitations on the period for which data is available. Data from the Magistrates Courts is only considered reliable for statistical reporting from 1 January 2004. Data from the Supreme and District Courts is only considered reliable from 1 March 2005.

Statistics kept by DJAG are available to the general public on request upon completion of a data request form, which is available at www.courts.qld.gov.au/media-and-the-public/courts-statistical-information. The Commission was told that data will be released to the public, provided it does not breach privacy restrictions and is not too resource-intensive to collate.

Statistics kept by the Department are also made publicly available when reported in the Annual Reports of DJAG and the Supreme, District and Magistrates Courts.

The Commission was also referred to data reported by the Australian Bureau of Statistics regarding Criminal Courts. Additionally, there is a database maintained by the Government Statistician’s Office, Queensland Treasury (see below). Data relating to criminal courts is kept by this entity. This data is sourced from the QWIC database, and is downloaded every two months. The data is cleansed by the Office and used to report annually to the Australian Bureau of Statistics. The cleansing process involves the data being checked for potentially incorrect information.

The Commission asked for statistics in respect of particular offence provisions, and the information was helpful to the extent that it set out the numbers of offenders, the courts before which they appeared and the types of orders imposed. The data does not, however, descend into the kind of detail required to assess the nature and extent of organised or networked offending in any particular area, or to form any view about future trends.


These statistics are taken from the Australian Bureau of Statistics data collection relating to Criminal Courts, Australia, 2013–2014, described above. The figures were provided to the Australian Bureau of Statistics by the Queensland Government Statistician’s Office in the first place. However, some of the offence categories have been combined. For example, sexual assault was combined with other offence categories—namely, abduction and dangerous or negligent acts endangering persons.

This combination gives an even less accurate picture of defendants who have been dealt with for sexual offences involving children than the original statistics supplied to the Australian Bureau of Statistics.
Joint report by the Australian Childhood Foundation and Child Abuse Prevention Research Australia, Monash University: They count for nothing: Poor child protection statistics are a barrier to a child-centred national framework, February 2014

This joint report underlines the inadequacy of reliable statistics that are available regarding the abuse and neglect of children. It makes the point that accurate data on this issue is essential in order for governments to make any headway in the area of protection of children.

In Australia, the report stated that:

...there is no high quality surveillance data system. It is almost impossible to know the magnitude of the child abuse and neglect problem, because there are no clear and uniform definitions of child abuse and neglect across jurisdictions. It is also almost impossible to know whether incidence of child abuse and neglect is increasing or decreasing because there is no consistent use of definitions over time.

The report referred to the ‘Child Protection Report’ produced annually by the Australian Institute of Health and Welfare, referred to above. The report stated that:

This report is the main source of publicly available data relating to state and territory child protection systems. However for more than ten years the report has warned that the data from the different jurisdictions are not comparable.

It is apparent that the problem of inadequate data on this topic applies across all Australian jurisdictions. It is also apparent that that problem impacts the capacity of policy and law-makers to properly understand the nature of child abuse and neglect, important for present purposes in the area of child sex offending.

It follows that it is impossible to state a firm conclusion on the prevalence of online child offending in the context of organised crime in Queensland. Having said that, and in supporting the need for an independent statistical body, it is tolerably clear from the information provided to the Commission by officers of the QPS and the CCC that the problem of online child sex offending in Queensland, and against Queensland children, is enormous and growing.

Recommendation

4.1 The Commission recommends that the Queensland Government proposed independent crime statistical body, once established, prioritise the collection and analysis of data relevant to organised crime in Queensland.

4.2.3 Victim impacts and impacts on the community

There can be no doubt that the impacts of sexual offending against children are often profound, with effects being felt in the short- and long-term:

The harm caused by child sexual abuse and organised child sex offending is complex. Depending on the circumstances of the abuse, an individual victim can experience severe life-long harm. Research demonstrates that psychological, physical and behavioural harms may be severe, extensive or long-lasting when the abuse involves the elements that are indicative of organised abuse. Family environments can also be severely damaged, which causes additional harm to victims.

It has been well documented that the sexual abuse of children has a range of very serious consequences for victims. Zwi et al. (2007) list depression, post-traumatic stress disorder, antisocial behaviours, suicidality, eating disorders, alcohol and drug misuse, post-partum depression, parenting
difficulties, sexual re-victimisation and sexual dysfunction as some of the manifestations of child sexual abuse among victims.50

Many studies have been conducted on the impacts on victims of child sexual abuse. For example, Lamont (2010)51 found that the consequences of child abuse and neglect include difficulties in forming relationships, poor physical health, learning and developmental difficulties, behavioural problems and mental illness. He also noted that other lifestyle consequences include an increased risk of developing drug and alcohol addictions, engaging in violence, criminal behaviour, long term unemployment and homelessness. Frederick and Goddard (2007)52 found that children who experience abuse and neglect are more likely, as adults, to experience poverty, disadvantage and exclusion.

Financial cost

In 2008, a report called ‘The Cost of Child Abuse in Australia’53 was jointly prepared by the Australian Childhood Foundation, Child Abuse Prevention Research Australia at Monash University, and Access Economics Pty Ltd. The report outlined the estimated financial cost to the Australian community of child abuse and neglect. Two different types of costs were calculated using two separate approaches. The calculations made throughout the report were chosen specifically to be inherently conservative in order to ensure that the final results were not inflated or disputable.

The first approach estimated the cost incurred by the Australian community associated with children who were abused or neglected in 2007. The final estimate comprised:

• the costs associated with the provision of health services to children who had been abused and neglected
• the identification and response to crime associated with the abuse and neglect
• the government expenditure on educational assistance to the affected children
• the estimated loss of lifetime earnings for those who survive their experience of abuse due to poorer labour market outcomes
• the government expenditure on care and protection
• a percentage of Supported Accommodation and Assistance Programs
• an estimate of the total cost of pain and suffering experienced in 2007 by the affected children.

The report stated that:

In 2007, it is estimated that 177,000 children under the age of 18 were abused or neglected in Australia. This figure could be as high as 660,000 children and young people. Based on these numbers, the best estimate of the actual cost of child abuse incurred by the Australian community in 2007 was $10.7 billion, and as high as $30.1 billion.

The second approach estimated the future costs to the community incurred over a lifetime for the children abused or neglected. This cost was calculated by forecasting the impact on children’s life outcomes across a range of measures for children abused or neglected for the first time in 2007.

The report concluded that:

In 2007, it is estimated that there were 130,237 children who were abused or neglected for the first time in Australia. This figure could be as high as 490,000 children. Based on these numbers, the projected cost of child abuse and neglect that will be incurred by the Australian community over the lifetime of children who were first abused or neglected in 2007 was $13.7 billion, but could be as high as $38.7 billion.

The Australian Institute of Family Studies—the Australian Government’s key research body in the area of family wellbeing—prepared a resource sheet published in September 2014 entitled, The economic costs of child abuse and neglect.54 The paper considered expenditure by federal, state and territory departments responsible for child protection services in Australia in relation to child abuse and neglect. The following
table provides an overview of real recurrent expenditure by state and territory governments and for the whole of Australia, for the 2012–2013 reporting period. The following amounts were spent directly on providing services to children who had experienced, or who were at risk of experiencing, child abuse and neglect in Australia. It is not possible to specify the amount spent on victims of sexual abuse alone.

Table 1: State and Territory

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>CPS</th>
<th>OOHC</th>
<th>IFSS</th>
<th>FSS</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>$11,929</td>
<td>$30,499</td>
<td>$961</td>
<td>$2,785</td>
<td>$46,174</td>
</tr>
<tr>
<td>NSW</td>
<td>$363,680</td>
<td>$766,849</td>
<td>$148,337</td>
<td>$123,077</td>
<td>$1,401,943</td>
</tr>
<tr>
<td>NT</td>
<td>$64,294</td>
<td>$76,483</td>
<td>$549</td>
<td>$35,316</td>
<td>$176,642</td>
</tr>
<tr>
<td>QLD</td>
<td>$307,900</td>
<td>$412,028</td>
<td>$40,390</td>
<td>$56,977</td>
<td>$817,295</td>
</tr>
<tr>
<td>SA</td>
<td>$51,867</td>
<td>$156,362</td>
<td>$10,995</td>
<td>n.a.</td>
<td>$219,224</td>
</tr>
<tr>
<td>TAS</td>
<td>$21,103</td>
<td>$41,967</td>
<td>$7,222</td>
<td>$4,829</td>
<td>$75,121</td>
</tr>
<tr>
<td>VIC</td>
<td>$198,500</td>
<td>$372,513</td>
<td>$66,805</td>
<td>$97,901</td>
<td>$735,719</td>
</tr>
<tr>
<td>WA</td>
<td>$128,239</td>
<td>$213,344</td>
<td>$28,876</td>
<td>$39,247</td>
<td>$409,706</td>
</tr>
<tr>
<td>Australia</td>
<td>$1,147,512</td>
<td>$2,070,045</td>
<td>$304,135</td>
<td>$360,132</td>
<td>$3,881,824</td>
</tr>
</tbody>
</table>

Notes: Units in $’000
CPS: child protection services; OOHC: out-of-home care; IFSS: intensive family support services; FSS: family support services.
Source: SCRGSP (2014) Table 15A.1

The resource sheet noted that Australian governments fund programs and services designed to prevent the occurrence of child abuse and neglect and to ameliorate the risk factors that contribute to child abuse and neglect. This expenditure is not included in the above figures, because it was difficult to specifically quantify expenditure on child abuse prevention activities. A further complication in the analysis is that many of the services funded to support and assist families may also assist to prevent child abuse and neglect.

It cannot be disputed that the impact on the victims of child sex offences is profound and affects many different aspects of their lives. The impact on the families of the victims as well as on the broader community are significant and far-reaching.

(Endnotes)

1 Transcript of Interview, Jon Rouse, 2 July 2015, p. 10
2 Section 210 Criminal Code.
3 Sections 349 & 208 Criminal Code.
4 Sections 215 & 217 Criminal Code.
5 Section 222 Criminal Code.
6 Section 229B Criminal Code.
7 Sections 299FA (obtaining prostitution from a person who is not an adult), 229G (procuring for prostitution), 229H (knowingly participate in the provision of prostitution) & 229L (permitting a person who is not an adult or has an impairment...
of the mind to be at a place used for prostitution) Criminal Code.


9 Information taken from the sentencing remarks of R v Brauer (Unreported, District Court of Queensland, Wall DCJ, 17 September 2014) and the sexual offences schedule provided by the Queensland Office of the Director of Public Prosecutions (response to notice 297173).

10 R v Kight (Unreported, District Court of Queensland, Samios DCJ, 26 August 2014); Schedule of facts and criminal history provided by the Queensland Office of the Director of Public Prosecutions in response to issued notice.

11 R v Goodwin (Unreported, District Court of Queensland, Shanahan DCJ, 23 May 2014) and R v Goodwin, Ex parte Attorney-General (Qld) [2014] QCA 345.


16 R v Baxter (Unreported, District Court of Queensland, Shanahan DCJ, 10 May 2013).

17 R v Sirianni (Unreported, District Court of Queensland Jones DCJ, 19 June 2014).


19 Crimes Legislation Amendment (Sexual Offences Against Children) Bill 2010 (Cth), Explanatory Memorandum, p. 8.


22 Portfolio Priorities Statement, Justice and Attorney-General, Education and Training, annexed to letter from The Hon. A. Palaszczuk MP, Premier of Queensland and Minister for the Arts to The Hon. Y. D’Ath MP, Attorney-General and Minister for Justice and Minister for Training and Skills, 19 May 2015.


33 Australian and New Zealand Offence Classification, Appendix 1 to 4513.0 – Criminal Courts, Australia, 2013–14.


37 Response to issued notice, Jon Rouse.

38 Response to issued notice, Jon Rouse.

39 Powerpoint Presentation, Cameron Burke, 23 July 2015, p.22; Statutory Declaration of Cameron Burke, 26 August 2015.
4.3 Child exploitation material market

4.3.1 Types of offending

Unlike more traditional types of organised crime, participation in the child exploitation material market by possessing, making and/or distributing material is usually motivated by sexual gratification, rather than by money. Nevertheless, when offending starts to involve sharing material with other like-minded ‘criminal entrepreneurs’ and procuring children for abuse to feed the market, it begins to accord with the changing notion of organised crime. The child exploitation material market is a good example of the ‘crime-as-a-service’ business model espoused by Europol.

Networks that are used to share child exploitation material vary in size and sophistication. Peer-to-peer platforms allow loosely connected users to grow their own collections and share with others. At the other end of the scale, enormous, hierarchical networks have been formed through the development of organised and sophisticated sites protected by the anonymity of the Darknet.
Each Australian jurisdiction, including the Commonwealth, administers laws relevant to the regulation of the burgeoning child exploitation material market. In Queensland, relevant offending is dealt with in both the Queensland and Commonwealth Criminal Codes.

**Queensland Criminal Code**

The Criminal Code (Qld) defines child exploitation material as material that, in a way likely to cause offence to a reasonable adult, describes or depicts a person, or a representation of a person, who is, or apparently is, a child under 16 years:

(a) in a sexual context, including for example, engaging in a sexual activity; or
(b) in an offensive or demeaning context; or
(c) being subjected to abuse, cruelty or torture.1

The bulk of online child exploitation material appears to involve real children of all ages, including infancy, ranging in severity from semi-nudity to rape, torture, and bestiality.2 The statutory definition, however, is deliberately broad, and covers computer-generated images and descriptions included in fictional writing.3

The Criminal Code (Child Pornography and Abuse) Amendment Act 2005 inserted offences into the Criminal Code (Qld) that are relevant to the manufacture, distribution and possession of child exploitation material. Prior to that, offences of this nature were found in the Classification of Computer Games and Images Act 1995, the Classification of Films Act 1991 and the Classification of Publications Act 1991.

As described below, the provisions of the Criminal Code (Qld) include a suite of offences covering conduct related to the making, distribution and possession of child exploitation material.

**Making child exploitation material**

Section 228A proscribes involving a child in the making of child exploitation material. A person involves a child in making child exploitation material if he or she:

(a) in any way concerns a child in the making of child exploitation material; and/or
(b) attempts to involve a child in the making of child exploitation material.

Section 228B prohibits the making of child exploitation material. The ‘making’ of child exploitation material includes the production of—and attempts to produce—child exploitation material.

Offending conduct that might attract a charge under section 228A is conduct commonly known as sexting (for example, sending sexually explicit images via mobile phone) when the child is under 16 years old.

The Commission is aware of the debate about whether teenagers should be the subject of criminal charges for what some describe as modern-day conduct undertaken by sexually curious children. Since such conduct falls outside of the Commission’s terms of reference, no view is expressed in respect of that debate. The reality is that the conduct does constitute an offence. The Commission was told that the Queensland Police Service (QPS) considers whether or not to lay charges in such matters on a case-by-case basis. Circumstances that might lead to criminal charges include the age gap between the parties to the ‘sexting’, and whether images or videos were distributed to others.4
Case study

R v MJC

MJC was a young man of 18 years who asked a 14-year-old girl to send him photographs of her breasts and vagina. MJC knew the girl from school, and made the request during an exchange of text messages. The girl sent one photograph of her breasts. MJC deleted the text messages, including the photograph.

MJC was embarrassed, remorseful and of otherwise good character. He was sentenced in the District Court and placed on a good behaviour bond for 12 months, and no conviction was recorded.

The more serious aspect of this type of offending is making child exploitation material which is then shared with others in the market (whether it was made with that purpose in mind, or otherwise). In the case of highly organised child exploitation material sites on the Darknet, production of new material is often a prerequisite to advancing though membership levels, and the fact of being a producer brings with it special status (see Case study: Shannon McCoole below).

Distributing child exploitation material

Distributing child exploitation material causes images of exploited children to be made available to the market, and often achieves for the offender the trust of others in a particular forum and a superior status in organised, hierarchical networks. Section 229C creates the offence of distributing child exploitation material, and in that section, to ‘distribute’ child exploitation material includes:

(a) communicating, exhibiting, sending, supplying or transmitting child exploitation material to someone, whether a particular person or not; and

(b) making child exploitation material available for access by someone, whether by a particular person or not; and

(c) entering into an agreement or arrangement to do something in paragraph (a) or (b); and

(d) attempting to distribute child exploitation material.

Possessing child exploitation material

In Queensland, the knowing possession of child exploitation material is an offence pursuant to section 228D of the Criminal Code. Although many offenders perceive their collections of child exploitation material to be satisfying their desire or fascination without committing any actual harm to children, it has long been recognised by courts in Queensland that possession of child exploitation material is not a victimless crime:

The production of child pornography for dissemination involves the exploitation and corruption of children who are incapable of protecting themselves. The collection of such material is likely to encourage those who are actively involved in corrupting the children involved in the sexual activities and who recruit and use those children for the purpose of recording and distributing the results. The offence of possessing child pornography cannot be classed as a victimless crime. The children, in the end, are the victims.

All of the child exploitation material offences (involving a child, making child exploitation material, distributing child exploitation material and possessing child exploitation material) carry a maximum sentence of 14 years imprisonment, and is subject to defences set out in section 228E.

The following case study provides an example of an offender who had engaged, possessed, made, and distributed child exploitation material. The categories of images refers to the classification system currently used in the criminal justice system to provide a breakdown of the number, type and level of depravity of child exploitation material in an offender’s collection. It is commonly known as the Oliver scale, and is
discussed in detail in Part 4.5 (Legislation) below. For present purposes, the Oliver scale is comprised of the following categories:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Images depicting erotic posing with no sexual activity</td>
</tr>
<tr>
<td>2</td>
<td>Sexual activity between children, or solo masturbation by a child</td>
</tr>
<tr>
<td>3</td>
<td>Non-penetrative sexual activity between adults and children</td>
</tr>
<tr>
<td>4</td>
<td>Penetrative sexual activity between children and adults</td>
</tr>
<tr>
<td>5</td>
<td>Sadism or bestiality</td>
</tr>
<tr>
<td>6</td>
<td>Anime, cartoon or virtual images</td>
</tr>
</tbody>
</table>

Case study

R v STK

In February 2012, Taskforce Argos officers were alerted by the Australian Communications and Media Authority to concerning images of young children on a file-sharing website. Officers discovered that STK was the person responsible for uploading the images to the website. He was identified through a number plate depicted in one of the photographs which had been uploaded. A search warrant was executed at STK’s residence, and officers seized an enormous quantity of child exploitation material in different forms. The material included:

- 32 videos which the defendant had taken of his two daughters in the bath or dressing, or close-ups of the girls’ genitals and breast areas. One daughter was aged 11 to 14 years and the other daughter was aged 8 to 11 years at the time of the recordings. The children were recorded when they visited the defendant following the separation of their parents. The recordings were made between January 2001 and December 2003. All the recordings were classified as Category 1 images. These recordings were the basis of the indecent treatment offences.

- A large quantity of videos, movies and still images compiled by the defendant and which all contained child exploitation material. He took movies of his own family members and also covertly recorded the neighbourhood children. The defendant took still images from movies, made them into slide shows, and then saved them to DVD. There were approximately 10 movies found of the neighbourhood children, which contained child exploitation material with the children in states of partial undress or in compromising positions.

- 43 narrated slideshows saved on DVD, VHS cassettes, SD cards, mini-cassettes or other tape forms. The defendant used the slideshows he had made and narrated child abuse stories to them. He also used adult pornography movies and narrated child abuse stories to them. Sometimes, he would use a child’s voice to act out the parts. The footage would sometimes cut to a still image of the child who was the subject of the story. The defendant would save these on various discs or DVDs. Ninety per cent of the narrations are to images or movies of girls under 12 years of age, and most of them were classified as Category 4.

- 24 cassettes or DVDs that contained compilations of the narrated stories or movies.

- 1,678 scrapbooked and collaged images made by the defendant. These were created from magazine pictures, stills taken from movies created by the defendant, or photographs in his possession. He edited the images to make them more sexually explicit by transposing cut-out
pictures from magazines or medical text books. The defendant had collected, for this purpose, unsold magazines from a newsagency where he had been previously employed.

- Two laptop computers which contained saved files of child exploitation material.
- 1243 handwritten stories, written by the defendant, which included stories of the defendant sexually abusing his children, nieces and nephews, fictitious children or neighbourhood children; or about children engaged in sexual activity with the defendant’s relatives. The stories included a description of anal, vaginal and oral sex with children. The majority of the stories were classified as Categories 3 and 4.

<table>
<thead>
<tr>
<th>Type</th>
<th>Total number</th>
<th>Unique number</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photographs/scrapbook images</td>
<td>1,678</td>
<td>-</td>
<td>1,482 – Category 1 7 – Category 2 58 – Category 3 124 – Category 4 7 – Category 5</td>
</tr>
<tr>
<td>Handwritten stories</td>
<td>1,243</td>
<td>-</td>
<td>344 – Category 1 109 – Category 2 553 – Category 3 169 – Category 4 68 – Category 5</td>
</tr>
<tr>
<td>Laptop computers – stills</td>
<td>20,714</td>
<td>15,523</td>
<td>Categories 1 to 6 with more than 12,000 unique files in Category 1</td>
</tr>
<tr>
<td>Laptop computers – movies</td>
<td>557</td>
<td>291</td>
<td>Categories 1 to 5 with 184 unique files in Category 4</td>
</tr>
<tr>
<td>DVDs</td>
<td>216</td>
<td>-</td>
<td>Categories 1 to 5 with the majority being in categories 1 and 4</td>
</tr>
<tr>
<td>Other types of tapes/ discs containing movies</td>
<td>73 movies</td>
<td>-</td>
<td>Categories 1 and 4 with the majority in Category 1</td>
</tr>
<tr>
<td>SD cards</td>
<td>4,706 images and movies</td>
<td>-</td>
<td>Categories 1 to 6 with 3,632 images or movies in Category 1</td>
</tr>
</tbody>
</table>

The defendant told police he began collecting and creating the various images in 2005 or 2006. The offence of distributing child exploitation material occurred over the period from 16 January 2012 to 9 February 2012. The defendant bought a new computer after Christmas 2011, and in January 2012, he uploaded child exploitation material of the neighbourhood children to a file-sharing website. This website is a free service that allows users to share photographs with other users. The defendant uploaded 482 child exploitation images to the website on eight occasions. The images were all classified as Category 1, and showed the neighbourhood children partially dressed, revealing their underwear. The rules of the website required users to post at least 12 photographs to enable them to access photographs of other users.
The defendant set up a special email account to obtain and distribute child exploitation material. This was a separate email account to the one he used to communicate with friends and family members.

After the defendant posted the first set of photographs, he was contacted by email by another user, who asked for nude pictures of the children depicted in the posted photographs. This person also attached two images of child exploitation material to the email. The defendant forwarded emails attaching child exploitation material to other users. In total, he sent 160 emails attaching child exploitation material, to 42 users of the website. The attachments contained a total of 2,830 images and 260 videos.

The defendant sent four emails to other users which contained a link and a password to a website where a zip file which contained 2,330 child exploitation images could be accessed. A significant proportion of these images were classified as Category 4 images.

By trading images with other users, the defendant was able to build up his collection of child exploitation material. He saved traded images to CDs, DVDs or onto his computers.

On 21 August 2013, in the Brisbane District Court, STK pleaded guilty to 32 counts of indecent treatment of a child; one count of possession of child exploitation material; one count of making child exploitation material, and one count of distributing child exploitation material. The offending period began in January 2001 and continued up to the date of arrest in February 2012.

STK received a head sentence of four and a half years, suspended after a period of 560 days, with an operational period of five years. That term was imposed with respect to the offence of distributing child exploitation material, which was accepted as being the most serious of the offences for which STK was sentenced. Lesser concurrent terms of 18 months and two years imprisonment were imposed with respect to all but one of the indecent treatment offences. He had been in custody since his arrest on 8 February 2012, and the period of 560 days was declared as time served in respect of the sentence. He was also made subject to a three-year probation order in respect of one of the indecent treatment offences.

His Honour Judge Dearden referred to mental health issues and drug dependency. His Honour also described the distribution of child exploitation material offence as the most serious, and referred to the fact that once images are released onto the Internet, they can never be retrieved. This fact compounds the impact of the abuse on the child, as each time the image is viewed by another person, in a sense, the child is abused again. By distributing the images on the Internet, STK permitted others to participate in the continuous process of re-abuse of the victims of this appalling trade.8

Commonwealth Criminal Code

Commonwealth legislation creates a number of offences relating to ‘child pornography’ material and ‘child abuse’ material. Although the terminology differs to some extent, the offences cover the same type of offending addressed by the Queensland Criminal Code. The Commonwealth Criminal Code also specifically deals with networked offending, whereas the Queensland Code does not.

‘Child pornography’ material refers to material that depicts the sexualised behaviour or sexual activity of an individual under the age of 18. ‘Child abuse’ material is concerned with material that offensively depicts or describes an individual under the age of 18 years who is the victim of torture, cruelty or physical abuse. When consolidated, the definitions of child pornography material and child abuse material cover the conduct included in the definition of child exploitation material in the Queensland Criminal Code (which includes the offensive depiction of the physical—whether sexual or not—abuse of a child).

Another difference between the Commonwealth and Queensland offences relates to the age of the individual the subject of the material. In Queensland, the definition of child exploitation material captures victims who are (or appear to be) under the age of 16. The definitions of child pornography material and child abuse material under the Commonwealth Criminal Code refer to subject individuals under the age of 18.9
Offending involving carriage services

Division 474 of the Commonwealth Criminal Code covers telecommunications offences. The purpose of the telecommunications-based child exploitation offences is to cover the range of activities that a person might engage in when using the Internet, email, mobile phones and other applications to deal with child pornography and child abuse material. These activities include viewing, copying, downloading, sending, exchanging material and making available for viewing, copying or downloading.

The telecommunications offences also deal with conduct involving the use of a carriage service to engage in sexual activity with a child, or causing a child to engage in sexual activity with another person. That type of offending is dealt with in this report above, under the heading of Online child sex offending.

Section 474.19 creates the Commonwealth offence of using a carriage service to access, cause material to be transmitted to a person, transmit, make available, publish, distribute, advertise or promote and solicit child pornography material. The maximum penalty is 15 years imprisonment.

Section 474.20 creates the Commonwealth offence of possessing, controlling, producing, distributing or obtaining child pornography material through a carriage service, and also carries a maximum penalty of 15 years imprisonment.

Section 474.22 is similar to section 474.19, but it relates to the use of a carriage service with respect to child abuse material. Similarly, section 474.23 is in identical terms to section 474.20 and also relates to child abuse material. In both cases, the maximum penalty is 15 years imprisonment.

Offences involving child pornography material or child abuse material outside Australia

Prior to the enactment of the Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010 (Cth), child pornography and child abuse material offences did not have extraterritorial effect. Division 273 now deals with offences involving an Australian citizen or permanent resident of Australia dealing with child pornography material or child abuse material overseas. The introduction of Division 273 recognised the transnational nature of online child sex offending, including the child exploitation material market:

Many countries do not have effective laws against child pornography and child abuse material, or lack the capacity to enforce them. This means that an Australian could travel overseas and make or purchase child pornography or child abuse material and escape punishment, even though the very same behaviour, if committed in Australia or through the Internet, would be a serious criminal offence.

Section 273.5 relates to offences of possessing, controlling, producing, distributing or obtaining child pornography material overseas. Section 273.6 deals with the same conduct, but in respect of child abuse material. Both offences carry a maximum penalty of 15 years.

Networked offending

The Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010 (Cth) also inserted sections 273.7 and 474.24A (the aggravated offences) into the Criminal Code (Cth). This was a significant step aimed at targeting involvement in child pornography networks.

The Explanatory Memorandum to the Bill explains that the Internet has allowed the development of organised, technically sophisticated rings of child sexual abusers. The purpose of the aggravated offences, which are directed at offenders who are involved in child pornography networks, is to reflect the increased levels of harm to child victims resulting from the demand created by such large-scale networks.

The aggravated offences automatically apply when the circumstances of the offence in regards to the following provisions suggest that the offence was committed as part of a network of offenders:

For offences committed by Australians overseas:

- Section 273.5 (possessing, controlling, producing, distributing or obtaining child pornography material outside Australia)
• Section 273.6 (possessing, controlling, producing, distributing or obtaining child abuse material outside Australia).

For offences committed in Australia:

• Section 474.19 (using a carriage service for child pornography material)
• Section 474.20 (possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service)
• Section 474.22 (using a carriage service for child abuse material)
• Section 474.23 (possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service).

The aggravated offences apply where a person commits one of the above offences on three or more separate occasions, and the commission of the offences involved two or more persons. The consequence of the aggravated offences is that the maximum penalty is increased from 15 to 20 years imprisonment.

Both aggravated offences provide that it is not necessary for the conduct constituting the aggravated offence to be the same on each occasion. That is to reflect the fact that offenders who are involved in criminal networks are likely to engage in several types of prohibited conduct. For example, a person might produce child pornography, distribute it to other members of a child pornography network and access child abuse material made available by other members of the network. Such an offender could be convicted of the relevant aggravated offence, notwithstanding the fact that they engaged in different forms of offending conduct on each of the three occasions. 13

In contrast, under the Queensland Criminal Code, there is no equivalent aggravated offence dealing with networked offending in the child exploitation material market.

4.3.2 Prevalence of offending

Like online child sex offending, the extent of offending—particularly organised offending—in the child exploitation material market is difficult to quantify. Aside from gaps in data collection and analysis, the reasons for this lacuna include the lengths to which users of child exploitation material go to ensure that the market is reasonably concealed from law enforcement authorities.

Also like online child sex offending, the online child exploitation material market is not new, but is evolving with the advancement of technology. The child exploitation material market is borderless and, as already mentioned, participants are historically early adopters of new forms of technology that increase efficiency and anonymity. Those factors contribute to an ever-expanding market where offenders are difficult to detect, locate and prosecute.

As far back as 2008, it was estimated that there were between 50,000 and 100,000 sex offenders involved in organised pornography rings around the world, with one-third of those operating from the United States. 14 Those numbers are likely to have grown exponentially with technological advances in the ensuing years.

One sophisticated site on the Darknet, closed by police in 2014 and discussed in detail below, had 45,000 members at the height of its operation.

In Queensland, the total number of ‘computer-related’ sexual offences received for prosecution by the Office of the Director of Public Prosecutions (ODPP) during the 2013–2014 financial year was 1,712. That data is not distilled to provide a picture of the prevalence of child exploitation material-related offending compared with, for example, online child sex offending.

Statistics reported by the Commonwealth Director of Public Prosecutions (CDPP) for the same period provide a more detailed breakdown of the types of offending on a national level, but do not delineate offending on a state-by-state basis (see Table CDPP Annual Report Figures in the previous section of this report). The most prevalent type of offending across the country during that period was using a carriage service to access child
pornography. There were three Commonwealth prosecutions under the aggravated networking provision in section 474.24A.

The dearth of data available with which to draw conclusions about the prevalence of offending in the child exploitation material market—let alone about organised or networked offending in that area—further supports the need for an independent crime statistical body with a brief to monitor organised crime in Queensland, amongst whatever other functions it might hold.

Despite the lack of statistical data or formal analysis, the Commission became aware during the course of the Inquiry that the QPS and the Crime and Corruption Commission (CCC) are faced with a constant battle to keep up with—and preferably ahead of—offenders participating in the growing and increasingly sophisticated child exploitation material market. There are many challenges for law enforcement in policing this type of networked offending, as discussed in more detail in in the section titled Responses, below.

In efforts to gain as fulsome an understanding as possible about the nature and extent of organised crime in this area, the Commission required the attendance of the following individuals to provide information pursuant to s.5(1)(c) of the Commissions of Inquiry Act 1950:

- Detective Inspector Jon Rouse, Taskforce Argos, QPS
- Paul Griffiths, Victim Identification Coordinator, Taskforce Argos, QPS
- Detective Senior Sergeant Cameron Burke, Cerberus Unit, CCC

Mr Griffiths is a civilian employee of the QPS, having served as a police officer in the United Kingdom for 18 years. He has been investigating online child abuse since 1995, and commenced work as the Victim Identification Coordinator with Taskforce Argos in 2009. In his role, Mr Griffiths works to identify child victims depicted in child exploitation material that comes to the attention of Taskforce Argos. Mr Griffiths has been involved in various capacities with relevant groups within Interpol since 2003, and is currently the Chair of the Crimes Against Children Group.

When asked whether the QPS was seeing networked offending in this area, Mr Griffiths pointed out that since the Internet is, in itself, a network, anyone operating on the Internet is operating in a loose network. The Commission was informed of a number of modes of offending in the child exploitation material market that involve varying degrees of networked conduct.

Peer-to-peer file-sharing

File sharing of child exploitation material on peer-to-peer (P2P) platforms is a ‘very loose trade’ without the feature of organisation, although as Detective Senior Sergeant Cameron Burke demonstrated in his presentation to the Commission, its prevalence in Queensland—and across the globe—is alarming.

Peer-to-peer file-sharing is the distribution and sharing of digital files within a P2P network. A P2P network involves an interconnected network of users (peers) who share files amongst each other without an intermediate server. Each peer within the network is both an uploader and downloader of content in relation to other users. Put simply, individuals who engage in file-sharing make digital files available for upload to other unknown users of the file-sharing platform. Simultaneously, the same individual may also receive files by downloading files they wish to obtain onto their personal computer.

The network itself will transcend national and international boundaries. A simple ‘google’ search for peer-to-peer programs demonstrates that many exist. Programs are free to download and available to anyone with Internet access, anywhere in the world.

P2P file-sharing is usually anonymous, in that a user offering files for sharing (be they music, video, or child exploitation material files) will not know who has accessed their content.

An exception is sometimes seen in P2P programs that offer Friend-to-Friend (‘F2F’) as an additional service. F2F networks allow users to make direct, closed connections with specific known users. As a result, F2F networks often use authentication methods such as passwords or digital signatures.
P2P networks are popular forums for the distribution of child exploitation material because they are free and easily accessible by the general public with little or no technological knowledge. The anonymity of peers within P2P networks leads to an impression that the risk of detection is minimised.

Like other online technologies that have been adopted for the purposes of providing an online child exploitation material market, the nature and extent of the problem is difficult to quantify. Reasons include the lengths to which users of child exploitation material go to ensure that the market is reasonably concealed from law enforcement authorities. Nevertheless, an analysis of case law and arrest data in Queensland indicates that a significant number of child pornography users are detected on P2P networks, suggesting it is still commonly used by participants in the child exploitation material market.

An American study conducted between October 2010 and September 2011 tracked users downloading known child exploitation material files with a particular P2P file-sharing network. Using software available to law enforcement authorities, the researchers discovered that 244,920 computers in the United States had shared 120,418 files during this period. The Commission was unable to find a similar Australian study.

The following case study involves child exploitation material offender Schultz, a prolific user of P2P platforms. It demonstrates the volume of material being shared on such platforms and the depravity of the content. It is also a case where the aggravated (networking) offence under the Commonwealth Criminal Code was charged.

The case is at odds with the position taken by the QPS in respect of P2P offending. Deputy Commissioner Barnett told the Commission (and the sentiment was mirrored by officers from Taskforce Argos) that P2P investigations are not considered to be investigations that involve networking of offenders. Support for that suggestion is said to come from the terms of the aggravated (‘networking’) offence under section 474.24A, which was thought not to apply to P2P offending.

In fact, Schultz is one of a number of Queensland offenders who have been successfully prosecuted under the Commonwealth networking provision for offending within P2P closed networks. The case study also highlights the common situation where a combination of State and Commonwealth offences are charged. Less commonly, this case also features a combination of contact offences and child exploitation material offences, although the different types of offending were not related.

Case study

*R v Schultz [Unreported]*

In 2011, the then-Crime and Misconduct Commission undertook a covert operation within the P2P network. Posing as an individual seeking child exploitation material, the investigator was able to ascertain that an individual, using an alias, was making child exploitation material available for sharing. The IP address was traced to the residence of Timothy Schultz.

Forensic examination of the offender’s storage devices demonstrated that he had accessed and downloaded 48 child exploitation material files during a period of approximately eight months.

The offender used a programme which allowed secure encrypted P2P file-sharing and instant messaging. Schultz downloaded the programme in February 2011, and had 95 contacts as at February 2012.

Schultz downloaded material covering the spectrum of child exploitation material, from children (from infancy to age 12) naked or semi-naked in sexual poses, to images of penetrative sexual activity involving children (as young as three), to images and videos in the category of sadism, bestiality, or humiliation involving children (including a lengthy video featuring a boy of about nine years old, entitled ‘Kidnapped, drugged and raped’).

Schultz used Windows Live Messenger, an instant messaging service incorporating email, to chat with like-minded individuals and transfer material. He also used Skype and Hotmail (and perhaps Yahoo) to transmit child exploitation material.
The networking offence was established by forensic examination of Schultz’s account. Schultz had made child exploitation material available online to up to 94 users on 59 occasions. Schultz had configured his account in such a way as to give unrestricted access to those users, to the six folders he made available. Those folders contained 1,452 child exploitation material files. A third of that material was film (599 videos), showing children being degraded and abused for a long period of time. There were a large number of files in the worst categories of child exploitation material.

In addition to accessing material and downloading it, Schultz was found to be in possession of 3,191 child exploitation material images and 599 films, including 398 films in the most depraved categories.

In sentencing Schultz, Justice Atkinson made the following observations:

It is hard to understate the shocking nature of this material and the vicious exploitation of children involved in the production of this material. You did not produce it, but by watching it and by sharing it, you are part of worldwide exploitation of the most vulnerable people.

Schultz cooperated with authorities, including providing passwords for his accounts (although it was said they could have been independently ascertainable through forensic examination). Schultz also told investigating police about a sexual encounter with a 13-year-old boy in 2006. Schultz came to know the boy in a chat room forum, where the boy talked about being bullied at school. The talk turned to sex, and eventually the boy agreed to meet with Schultz. Sexual acts, including sodomy, were committed by Schultz, largely without complaint by the boy; however, Schultz did not desist when asked to during intercourse.

Schultz was 26 years old with no criminal history and had held a blue card. He pleaded guilty to the following five offences:

- Using a carriage service to access child pornography material: section 474.19 of Criminal Code Act (Cth)
- Using a carriage service to transmit, make available, publish, distribute, authorise or promote child pornography material (two counts, relating separately to the use of each account): section 474.19 of Criminal Code Act (Cth)
- Making available child pornography on three or more occasions to two or more people (the aggravated ‘networking’ offence): section 474.24A Criminal Code (Cth)
- Possessing child exploitation material: section 228D of Criminal Code (Qld)
- Two counts of indecent treatment of a child under the age of 16: section 210 of the Criminal Code (Qld)
- Unlawful sodomy: section 208 of the Criminal Code (Qld)

On 19 March 2013, Schultz was sentenced to an effective term of imprisonment of six years with an order that he be eligible for parole after two years.

Using the Surface Web – forums and email communication

Another mode of offending seen by police in the child exploitation material market is more organised in the sense of offenders seeking out like-minded others, but less prevalent. A user on an open forum might glean a shared sexual interest in children of another user through innuendo or euphemism on that forum, and thereafter move their communication to email or some other form of direct communication. In that way, the offenders form a small network within which they trade material.

This mode of offending uses the Surface Web, also known as the open Internet or Surface Net. The Surface Web encompasses the Internet as the typical Internet user would understand it—that is, anything that a search engine such as Google will index.
Online child sexual offending & child exploitation material

The Surface Web plays a slightly different role in child pornography offending. Serial offenders understand that online activities can be traced, and therefore will refrain from posting or sharing information on the Surface Web. Instead, the Surface Web has been identified as a point of contact for offenders. News groups, message boards and chat rooms are often used by offenders seeking others to discuss similar interests or share material. Once contact has been made, offenders will typically move to a more private arena, such as a F2F platform or through anonymous Darknet browsers like Tor, to trade and discuss material.

Child exploitation sites have been known to operate on the Surface Web. One notable example, detailed in the case study below, is that of Azov Films. That was a website ostensibly for the benefit of naturists and nudist enthusiasts. Police discovered that the content typically featured young males and was used as a portal for child exploitation material offenders.

Case study

Operation Spade

In May 2011, the Toronto Police Service Child Exploitation Section commenced Operation Spade after receiving numerous complaints from the public. The Operation involved the investigation of three websites: Baikal Films, Movie Bizz and Azov Films. The three websites operated under the umbrella of 4Point5Productions (4P5P), where Azov Films was identified as the main website.

The website itself operated like most other online stores: customers were able to browse categories or search for items using specific keywords. Each film was advertised on its own page with a photo of the DVD cover, a description and credits for the film with an option to view a complementary trailer before purchase.

Upon purchasing a film either by credit card or money order, a customer could choose to either download the film directly by clicking on a link emailed to them, or have a physical copy shipped to their address. If a file was downloaded, a unique hash algorithm was recorded, allowing Azov Films to trace anyone sharing unauthorised copies of their films. Azov films advertised their product as ‘legal’ and ‘naturalist’; however, the website issued a threat that the company would report a purchaser as a paedophile if it were discovered that the purchaser had shared the product.

A search warrant was executed on 4P5P, discovering an enormous business enterprise responsible for the operation of Azov Films, including the website servers. In addition to computers, DVD-burning units and video equipment, Canadian authorities seized 40 terabytes of digital data, including thousands of commercially produced child pornography DVDs featuring young boys.

Further investigation of the material found that many of the boys featured in the films were from the Ukraine, Romania and Germany, and most, if not all, parents were provided with financial incentives to make their children available for the films. It was also found that neither the parents nor the child ‘actors’ were permitted to see the footage, and customers from the Ukraine or Russia were blocked from accessing the website. The operation resulted in the rescue of over 400 children around the world.

Further analysis of the data identified a database of customers who had purchased material from Azov Films. This information was disseminated to the QPS directly from the Toronto Police. Upon receipt of this information, Taskforce Argos commenced an operation which resulted in many arrests. Ten per cent of all arrests were made in Queensland.

During the arrest phase of operation, an Argos investigator identified an offender, TM (see Case study: R v McCoole below), as having accessed a Darknet child pornography website. It was this discovery that commenced another operation, and which ultimately led to the arrest and conviction of Shannon McCoole.
Networks on the Darknet

At the top of the hierarchy of organised offending in the child exploitation material market are sophisticated websites dedicated to the proliferation and distribution of child exploitation material. These sites exist on the Darknet and, less commonly, on the Surface Web. They operate with an organised structure including a hierarchy of users, producers and administrators. In the majority of cases, members of such sites work together as a team, recruiting producers, trying to discover the whereabouts of victims, and sharing information about how to avoid detection.25

As to the prevalence of that type of highly organised offending in the child exploitation material market, Mr Griffiths, of Taskforce Argos, is of the view that while one might expect Australia to harbour a small proportion of offenders, behind countries like Russia, Brazil, Germany and the United States, it seems that ‘we have more than our share of higher level users of Darknet and Tor networks.’ That view is based on involvement in international operations revealing a number of Australians operating as administrators of popular Tor sites for new material; however, Mr Griffiths stressed that there is no reliable statistical data.26

Support for that view is found in the recent South Australian case involving a child sex offender who was also found to be the administrator of a highly networked child exploitation material sites operating on the Darknet. The Commission learned that Taskforce Argos was instrumental in identifying the offender as the administrator and, ultimately, in shutting down the site. At its height, the network had more than 45,000 members.

Case study

R v McCoole27

Shannon McCoole was convicted in South Australia of a range of sexual offences against children and child exploitation material offences under the Commonwealth Criminal Code, including the aggravated ‘networking’ offence. There were seven victims of sexual abuse, including boys and girls between eighteen months and three years. Most were in the care of the State in South Australia, and some had already suffered neglect. McCoole was also found to be the head administrator of an organised and hierarchical network operating a Darknet site devoted to child exploitation material on Tor.

McCoole had been employed by Families SA and Nanny SA from 2011 to 2014, in roles including ‘primary care, behavioural control, household duties and general transportation’. The self-confessed paedophile had been working in a government-run residential facility in-and-out-of-school care service.

Amongst the more than 50,000 images of child pornography found on McCoole’s computer was a cache of images and video files depicting his physical offending against the children. In chat logs found on his hard drive, McCoole had boasted about the offending. Amongst that chat, McCoole had talked about changes in opportunities to offend, had given advice about grooming and the benefits of sexual offending against younger children to other offenders.

McCoole came to the attention of authorities through international cooperation. In 2014, the Dutch Police contacted Taskforce Argos investigators in Queensland, having found a large quantity of child exploitation material during the course of their investigation of a child abuse website. Much of that material appeared to have been produced by a particular user (username X for the purpose of this case study) and had been circulated between an exclusive group of Tor users for their own private use. As it happened, police within Taskforce Argos had been monitoring the same website and were attempting to identify user X. Their interest had been sparked in mid-2013 when they arrested a paedophile during a separate investigation and discovered that he was a VIP member of the site.

Paul Griffiths, Victim Identification Co-ordinator with Taskforce Argos, set about analysing the information available in relation to user X. It was discovered that this person habitually used an unusual greeting in
online communications. By searching the Surface Web for other instances of this greeting, Mr Griffiths was able to identify McCoole as user X. The use of meta data allowed police to trace McCoole to South Australia, and law enforcement officers there were informed. A coordinated effort resulted in McCoole being arrested shortly thereafter. Detective Inspector Jon Rouse of Taskforce Argos said that ‘The Darknet areas are perceived as being safe for the sexual exploitation of children. The work performed by Argos Detectives through this operation has proven that is not the case.’

Following McCoole’s arrest, Argos Detectives continued to work to shut down the producers’ section of the site in order to protect children from further harm while they continued the investigation. Ultimately, with the assistance and cooperation of international law enforcement agencies, the site was shut down.

Features of the Tor-based Website

The website had a hierarchy of membership broken into rankings or authority levels. The head administrator was Shannon McCoole. Under him, were four website administrators. The next group down in the hierarchical structure were co-administrators, and under those people were ‘moderators’. These roles comprise what was called the ‘admin team’.

Each admin team member had a role detailed by the head administrator, and each co-administrator had one or two roles—again determined by McCoole. The moderators had the task of assisting with the moderation of the posts, checking them to make sure they were properly completed and in accordance with the rules. Members were sanctioned if the rules were not obeyed. Sanctions included warnings, temporary bans, permanent bans and deletion. All admin team members had access to all areas of the board.

The site had several membership classes; registered members, full members, VIP members and SVIP members.

Outside of the membership hierarchy, there were two parts of the site only accessible to certain members:

- The private zone – reserved for new or rare content. To gain access, lower status members were required to post their new or rare content, and existing private zone members would vote to decide whether it was new or rare enough to grant membership. While the content did not have to be produced by the member, it must not have been in wide circulation. Members of the private zone were required to post every 14 days to maintain their membership of that private zone.

- The producer’s lounge – for members who were producing their own content. In order to gain access to the producer’s lounge, a member must have proven that he or she has access to at least one child, and the ability to produce content involving that child. The content was required to contain penetration of the child and the use of a particular specified object to prove recent production and authenticity. Videos were required to be at least five minutes in length, or at least 100 images were to be provided. It was a further requirement that the child hold a sign that had the applicant’s user name and the date and particular words for further authentication of the production. Producers were required to post every 14 days to maintain their status.

For his role in the administration of the site (which attracted an aggravated ‘Networking’ charge) and for his sexual abuse of children, McCoole was sentenced on 7 August 2015 to 35 years imprisonment with a non-parole period of 28 years.

One of the most concerning aspects of these types of organised criminal networks is the voracious demand for new and increasingly depraved material. The following case involved a VIP member who was required to contribute a certain amount of new material in order to maintain his membership status.
**Case study**

*R v TM*

TM was a Queensland man identified as a VIP member of the Darknet site administered by McCoole in 2013. His identification was the result of an international operation commenced by the Toronto Police Service in conjunction with the Royal Canadian Mounted Police and the United States Postal Inspection Service. As mentioned in the case study involving the Azov films website, information was sent by the Toronto Police to the QPS.

As a VIP member, TM was required to upload material on a monthly basis. His collection of child exploitation material was stored on two external hard drives and a personal computer containing a partitioned hard drive. One of the partitions was encrypted and the other was accessible. The entire collection was revealed as follows:

- 95,857 Category 1 images of which 84,851 were unique
- 26 Category 1 movies
- 1,147 Category 2 images of which 1,024 were unique
- 241 Category 2 movies of which 226 were unique
- 585 Category 3 images of which 567 were unique
- 39 Category 3 movies of which 38 were unique
- 562 Category 4 images of which 534 were unique
- 199 Category 4 movies of which 195 were unique
- Three Category 5 images
- One Category 5 movie
- 161 Category 6 images.

TM was charged with the following offences:

- Using a carriage service to access child pornography material: Criminal Code (Cth)
- Using a carriage service to transmit, make available, publish, distribute, authorise or promote child pornography material: Criminal Code (Cth)
- Possessing child exploitation material: Criminal Code (Qld)

He was sentenced in the District Court at Brisbane to a term of 30 months imprisonment, suspended after six months, for an operational period of 30 months.

The operation of the site featured in both case studies was undoubtedly an organised criminal enterprise. It had thousands of active members from all over the world, conspiring to assist each other in the commission of offences. Members had clearly defined roles, codes of conduct and a hierarchical structure. Its demise was largely due to the work of officers at Taskforce Argos, which is discussed in more detail below.

Beyond the demand for new material, the child exploitation material market is seeking material involving younger and younger children, and the market for ‘hurt core’ material (depicting rapes and violence, including killings) is bigger than ever before. Mr Griffiths informed the Commission that he knows of cases where offenders plan the abuse of children before they are even born. The well-publicised case of Newton and Truong is an example of a case involving the sickening abuse of a child adopted for that purpose. Images of the sexual abuse of the child became fodder for the market.
Operation Juliet Conduit (Newton and Truong)\textsuperscript{30}

This operation began in October 2011 and investigated the conduct of two former Queensland residents partners Mark Newton and Peter Truong. They illegally adopted a baby boy from Russia with the purpose of sexually exploiting him across a global network of child sex offenders. The two offenders operated within the Surface Web and used peer-to-peer platforms to connect with other like-minded offenders who were part of a computer-based group called the Man Boy Love network. They operated a sophisticated and heavily encrypted online network that hid the identities of the individual members. Before the boy turned 2 years old, the two men had committed sexual offences on him. He was taken to America and Europe multiple times, and handed over to other male sexual offenders who committed offences against the boy. There were at least eight other men involved in the sexual exploitation of the boy, across Europe and the United States.

The investigation commenced when a classification officer with the Department of Internal Affairs in New Zealand conducted a peer-to-peer investigation and consequently raided the home of a suspected child sex offender in Wellington. Officers found a cache of images of a young boy, none with an overt sexual flavour, but all depicting the child deliberately posed for the photographs. Investigating officers were concerned about the overtones to the collection and began a search for the child, wondering if the child’s parents were aware of the photographs being taken. There was also a collection of movie files, seemingly innocent on the face of them, showing the young boy with the offender and two other men, later identified as Newton and Truong, exploring caves and in other nature settings. A car with a Queensland number plate was captured in some of the footage, and Queensland detectives were asked for assistance. Taskforce Argos became involved in the enquiries, and this led them to identify Newton and Truong. Background checks on the two men revealed no criminal history for either of them. They lived in Cairns, and one was a photographer and the other was in the IT field.

Meanwhile, New Zealand officers dug deeper into the computer files of their suspect and uncovered the offender’s chat logs on Skype, which mentioned ‘Mark’ and ‘Peter’. The logs made direct reference to a group of offenders accessing a young boy for sex. Chat logs revealed that Peter was about to take a young boy to Germany and swap him with another boy for sex. There was also a mention of a trip with the boy in the following year to the United States.

The chat logs also revealed communications from two men in the United States and one in Germany. Enquiries by Taskforce Argos officers with United States authorities revealed that one of the American men, Edward De Sears, had already been arrested and charged with offences arising out of his involvement with a peer-to-peer network following an investigation by the FBI. Taskforce Argos officers made enquiries with the German police, and discovered that the German man, Hessler, was also in custody for child abuse charges. Hessler had a young son who provided information to the German police that he had met the boy who had two dads, in Germany.

Enquiries by Taskforce Argos revealed that Newton and Truong had just left Cairns, with the boy, for an extended stay in Los Angeles, and the search was on to find the boy. Inspector Jon Rouse, Taskforce Argos, contacted a colleague in the United States with the USICE (United States Immigration and Customs Enforcement) who arranged for some enquiries to be made with the Los Angeles Police Department.

Simultaneously, Taskforce Argos officers executed a search warrant on the residence of Newton and Truong.

Police officers found a passport belonging to the boy. At this point, the little boy was only 6 years old and the passport in the house was filled with travel entries. Police officers found an extensive range of hard drives and other computer storage devices. Some material was able to be accessed, but a large proportion of it was encrypted. Police found some negatives of photographs taped into the back of a book, which
showed images of child exploitation material not relating to the boy. It was apparent that there were many photographic and video recordings of the boy with the men both at home and travelling, which could be viewed by police, but none of it amounted to child exploitation material. It was material that any family might have in their family albums.

In the United States, while driving in Los Angeles traffic, Newton and Truong were arrested by American police officers and taken into custody. The boy was not with the men at the time of their arrest. The boy was located and interviewed. He made no disclosures of sexual abuse to police; however, it was suspected by officers that he had been coached in how to respond to certain types of questions. For example, he said he knew Newton and Truong; he was bright and responsive when asked non-contentious questions; however, he was non-responsive to specific questions about sexual abuse and expressed a concern that his parents would go to gaol. There were computer devices in the possession of the two men at the time of their arrest, but the data on those was also encrypted. The men declined to be interviewed.

Unfortunately, with no disclosures by the boy, no admissions by the men, and no evidence located on computer devices, there was insufficient evidence in the view of United States law enforcement agencies to charge the men with any criminal offences. There was, however, a sufficient basis to keep the boy in care, subject to further enquiries. Taskforce Argos officers were under pressure to locate evidence to charge the men. Meanwhile, Newton and Truong used the media to their advantage, and maintained they were being targeted because they were homosexual fathers. They took part in an interview aired on United States radio and maintained their innocence, citing it as coincidence that the three men they had happened to innocently visit (De Sears, Hessler, and the New Zealand man) were also in custody over child pornography charges.

Mr Paul Griffiths, of Taskforce Argos, had the enormous task of combing through all the seized computer-based evidence taken from the Cairns residence of Newton and Truong. Mr Griffiths began the task of compiling a timeline of the Skype communications that had been captured by police. He also filled in the timeline using information gathered from the family photographs and recordings taken by Newton and Truong showing the boy growing up and travelling. The resulting timeline showed the travels of the three around the world. Mr Griffiths sifted through nearly 300,000 images and 5,200 videos.

Taskforce Argos officers sent the images and recordings to Washington DC, to assist with the investigation there.

At the same time, Inspector Bone of the United States Postal Inspection Service (based in Washington DC) independently uncovered a hidden network of child sex offenders operating an Internet relay chat group called ‘Tail of the Dragon’. This was a case also involving the Toronto Police Service. The network had operated for over two decades around the world, trading millions of photographs and videos depicting young boys. It used a file transfer protocol to send child exploitation material to its members. It was a sophisticated network, built by its members—some of whom were highly skilled IT professionals—who used encryption to thwart detection by law enforcement agencies. Peter Truong was discovered to be a member of the group, operating under the pseudonym, RedRover.

A United States offender led police to a person known on the network as ‘The Beav’, who had shared material that depicted the boy with others on the network. The images showed a mole on the stomach of the boy, and also featured the Beav sexually abusing the child. Inspector Bone overheard a conversation amongst police officers talking about the case from Australia. He asked to look at the images that had been sent by Taskforce Argos.

The boy, who had received a distinctive temporary henna tattoo on the trip and also had a mole on his stomach, was identified in stills of videos which had been discovered in the United States police investigations. The footage captured sexual offences being committed on the boy. Inspector Bone was able to tie the child portrayed in the images featuring the Beav to the images sent by Taskforce Argos. Police then had evidence to charge the two men with sexual offences against the boy as well as their roles in the network. Taskforce Argos officers trawled through the images taken from the Cairns house and were able to identify the Beav in some of those images.
Prior to his sentence hearing, Truong provided police with the passwords and codes to his encrypted files. This provided more evidence regarding the sexual abuse of the boy.

In 2013, in the United States, Truong—an Australian citizen—pleaded guilty to the offences of conspiracy to sexually exploit a child and possess child pornography, and Newton—a United States citizen—pleaded guilty conspiracy to sexually exploit a child and conspiracy to possess child pornography. Truong was sentenced to 30 years imprisonment, and Newton was sentenced to 40 years imprisonment.

A Queensland man was also arrested and charged as a result of the investigation of Newton and Truong. He pleaded guilty to the Commonwealth offences of using a carriage service in an offensive way and using a carriage service to transmit child pornography material. He was not charged with contact offences against the boy, but had transmitted some images of the boy over Skype. He was an associate of Newton and Truong and was employed as the director of a child care centre in Queensland over some of the period of the offending. This man had travelled with Newton and Truong to the United States and was with them when they were arrested.

It was a combination of dogged police work and luck—together with effective cooperation between officers attached to Taskforce Argos, the New Zealand Department of Internal Affairs, several United States law enforcement agencies and the German police—which led to the ultimate arrest of Newton and Truong.

The preceding case is a staggering example of the level of sophistication of criminal networks committing sexual offences against children, all aided by technology available as a result of the Internet. It also underpins the importance of law enforcement agencies working together across the globe.

The QPS and the CCC have on their hands a constant battle to keep up with—and preferably ahead of—what offenders are doing, and acknowledge the difficulty of overcoming the anonymity of individuals who use the Darknet.

Offender typology

The types of participants within the networked online child exploitation material market tend to vary, based on the extent of their participation. Krone identifies a number of categories of offender which relate to online child exploitation material-related offending. Typical categories of offender include:
<table>
<thead>
<tr>
<th>Type of Involvement</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>Accidental possession of child exploitation material. Material knowingly saved.</td>
</tr>
<tr>
<td>Private Fantasy</td>
<td>Conscious creation of text or digital images for private use.</td>
</tr>
<tr>
<td>Trawler</td>
<td>Actively seeks child exploitation material using public websites.</td>
</tr>
<tr>
<td>Non-Secure Collector</td>
<td>Actively seeks material often through P2P networks.</td>
</tr>
<tr>
<td>Secure Collector</td>
<td>Actively seeks material but only through secure networks.</td>
</tr>
<tr>
<td>Groomer</td>
<td>Cultivating an online relationship with one or more children. Pornography may be used to facilitate abuse.</td>
</tr>
<tr>
<td>Physical Abuser</td>
<td>Abusing a child who may have been introduced to the offender online. Pornography may be used to facilitate abuse.</td>
</tr>
<tr>
<td>Producer</td>
<td>Records own abuse or that of others (or induces children to submit images themselves).</td>
</tr>
<tr>
<td>Distributor</td>
<td>Distributes child exploitation material.</td>
</tr>
</tbody>
</table>

The motivators of individuals can be further categorised. Research suggests that individuals who access the online child exploitation material marketplace can be classified as follows:

- individuals with a genuine sexual interest in prepubescent children or adolescents; child exploitation material is accessed for sexual fantasy and/or gratification
- individuals with a passing sexual curiosity in child exploitation material who download minimal amounts to satisfy that curiosity
- individuals who are constantly seeking new and different sexual stimuli.13

Regardless of the category of offender, all participants in the child exploitation material market unequivocally contribute to, and stimulate demand for, new material from producers. In this way, all participants contribute to the proliferation of the market.

### 4.3.3 Victim impacts and impacts on the community

#### Victims

The online child exploitation material market has a significant detrimental impact on the community as it stimulates the demand for production of child exploitation material and therefore promotes child sexual assault. In addition, beyond the impact of contact offending recorded for dissemination in the child exploitation material market, it is well known that victims of exploitation for the production of material for the market often suffer ongoing harm. The impacts on victims of child sexual abuse, as well as on their families, have already been set out in some detail in the section on online child sex offending, above.
Purveyors and collectors of child exploitation material commonly justify their actions by citing the explanation that they are not responsible for the level of trauma caused by contact offenders who produce the material. However, victims of exploitation often report deeper psychological trauma than victims of contact offending that remains private. That is because the number of images being circulated online and the number of recipients is ultimately unknown. This phenomenon effectively prolongs the abuse, and it is commonly reported that victims claim an ongoing belief that the child exploitation material of which they are a subject is being viewed by an individual at any given point in time.

That belief is far from fanciful in this digital age, and might be exacerbated by those in law enforcement and the criminal justice system having access to, and viewing the material. That is recognised in the Criminal Code (Qld), which excludes non-essential people from the courtroom when child exploitation material is on display. Section 229F requires the court to consider the public benefit of limiting the number of people with access to child exploitation material.

Financial cost

The financial costs discussed in the section on online child sex offending apply equally here. While many children who are abused in the making of child exploitation material live overseas, those who do live here suffer the same kinds of trauma (possibly even deeper trauma as mentioned above) and require the same kind of ongoing social, psychological and medical care that attracts a cost to the community. That cost is impossible to quantify.

The cost of policing and prosecuting this type of organised (in the sense of networked) crime is also significant.

The community

Some of those who work in the criminal justice system, including law enforcement authorities, are exposed to child exploitation material during the execution of their duties. Those people include police officers (especially those tasked with classification of images and victim identification), lawyers, judicial officers and administrative staff. Jurors who are selected to decide contested child exploitation material cases are also required to look at distressing material. Police officers with the QPS and the CCC are also required to pose as children and predators in the course of their covert work. That work, and exposure to child exploitation material, puts those working within the system at potential risk of psychological harm.

For that reason, organisations such as the QPS, CCC, and the CDPP have implemented policies and procedures to protect the psychological well-being of those individuals who are required to view child exploitation material as part of their work.

Queensland Police Service

The QPS also has a number of policies in place for employees who are required to view child exploitation material. The QPS policy documents expressly acknowledge that such roles expose members to behaviour and aspects of human nature not ordinarily experienced in other areas of policing.

Standing Order No. 6 of 2010 provides for a number of protective measures specifically for members of the Child Safety and Sexual Crime Group. Those measures include:

- A voluntary application process, whereby all sworn members are required to apply for a vacancy within the group. The advantage of this approach is to indicate a willingness to undertake the duties associated with the position.
- All sworn applicants are required to undertake psychological assessment prior to commencing duties to ensure suitability for working within the group.
- All sworn applicants are required to make themselves available for psychological assessment upon request on an ongoing basis. For those officers within Taskforce Argos, psychological assessment is also required on a six-monthly basis and upon exit from the online investigation group.
• Senior management is required to formally address each induction group to reinforce the strong commitment to the ongoing welfare of personnel involved in the group.

The Standing Order also includes a policy to ensure that, as far as practicable, officers will not be required to view more than four hours of child exploitation material per shift. In addition, in instances where it is clear that working within the group is adversely affecting an officer’s health, senior management will negotiate the transfer of the officer to another area within the service.

Crime and Corruption Commission

Police officers in the Cerberus Investigation Unit (Cerberus) are required to view and categorise child exploitation material as part of their duties. In covert operations, some police officers masquerade as children or predators. The CCC has a program designed to provide psychological assessment and support to those officers (and others working at the CCC).

This Commission was provided with the Psychological Assessment Program Policy and Procedure. It contains a number of protective measures including the requirement for a psychological assessment prior to commencing work within Cerberus. The procedure tailored for officers working in Cerberus (the Cerberus Psychological Assessment Procedure) provides for regular assessments, every six months, and debriefing as required.

Cerberus officers (including Civilian Categorisation Officers) are to perform their duties during daytime hours (unless approved otherwise) on no more than four days per week. After 400 contact hours, an officer must undergo psychological assessment regardless of whether six months has transpired since the last assessment.

The procedure provides for rotation of officer after three years (for police officers) and 18 months (for civilian employees). In addition there are a range of services made available, including the QPS occupational psychologist, chaplain and union.

Commonwealth Director of Public Prosecutions

The CDPP has a tiered approach to the management of employee wellbeing, which has a preventative and remedial focus. The CDPP Employee Wellbeing Program, Wellbeing Check – Fact Sheet and Director’s Litigation Instructions No.20 – Child Exploitation Material – Work Health and Safety Issues were provided to the Commission. The website articulates the purpose of the relevant procedures and guidelines:

Dealing with (child exploitation material) material requires investigators, prosecutors and courts to hear or read stories of a disturbing nature and may involve viewing pornographic material depicting explicit sexual acts involving serious harm to children. The CDPP has developed an Employee Wellbeing Programme designed to implement practical policies and guidelines to support employees who may be at risk of experiencing trauma as a result of exposure to potentially distressing materials.

The program includes the following protective measures:

• Monthly one-on-one ‘coaching conversations’ with new employees in areas that deal with potentially distressing case materials during the first six months of employment.
• A mandatory initial wellbeing check for legal and non-legal employees working in areas that may deal with potentially distressing case materials. The check is conducted by an experienced psychologist to determine the employee’s personal resilience, identify personal risk factors and advise on specific coping strategies.
• A mandatory wellbeing follow-up one to two months after the initial wellbeing check. This follow-up is intended to identify any undetected or emergent issues that have arisen after a period of exposure to potentially distressing material.
• Group-based wellbeing review sessions that are conducted at 12-monthly intervals for all employees undertaking work in areas that deal with potentially distressing materials.
• A formal standing ‘opt-out’ option for employees having spent two years working in a relevant area.
• Regular workload reviews.

The CDPP ‘Online child exploitation conduct of matters guidelines’ deals with matters such as the appropriate number of hours an individual may view materials, protocols as to when and where materials may be viewed, and guidelines on viewing disturbing materials safely. Where possible, CDPP officers should limit viewing time to three hours in any one sitting and breaks are encouraged. Material should be viewed in the first part of the day where possible.39

Office of the Director of Public Prosecutions (Qld)

The Queensland ODPP informed the Commission that the QPS holds primary and sole responsibility for the classification of child exploitation material in prosecutions. The ODPP would not assume responsibility for the conduct of a prosecution unless all images had already been classified, or if that had not yet occurred, the agency responsible for classification was the QPS (as opposed to a Commonwealth agency).

Although there are no circumstances where ODPP staff are required or expected to classify child exploitation material, the Director of Public Prosecutions has acknowledged that there have been a number of instances (approximately ten) where ODPP staff have classified a small number of images of their own volition.40 Having learned of those small number of cases, the now-Acting Director of Public Prosecutions stated his intention to remind staff that classification of images is not the responsibility of the ODPP and they ought not do it, whether the number of images is small or large, and whether or not that prevents court timelines being met.

Understandably, since the ODPP is not responsible for classifying images, and staff should not engage in such a task, there is no training provided in respect of the classification process. However, staff engaged in the prosecution of child exploitation material offenders are necessarily exposed to such material. While no measures have been put in place specifically concerning the risk of psychological harm to staff (because staff are not required to classify child exploitation material), the Commission is told that staff are routinely reminded of a free and confidential counselling service available to staff through the Department of Justice and Attorney-General’s Employee Assistance Service.41

Legal Aid Queensland

Legal Aid Queensland (Legal Aid) does not have a specific policy or guideline to address potential psychological harm to staff members required to view child exploitation material.

However, Legal Aid does have policies and procedures that aim to mitigate risks to staff members arising from their employment. Legal Aid acknowledges that there is risk of psychological harm by exposure to material relating to offences of violence, sexual offences, child abuse, and domestic and family violence.

The Risk Management Framework includes a procedure for assessing risk in the workplace and taking action to eliminate or minimise the possible consequences of such risks. Risks are recorded in a Risk Register, which is monitored by the organisation. The current controls for risks include:

• free counselling for employees
• regular training in respect of vicarious trauma and resilience
• staff trained in mental health first aid
• information available on the website outlining various resources available for support.

Legal Aid staff are also able to access services provided by the Queensland Government Employee Assistance Scheme.42
Jurors

The Department of Justice and Attorney-General, through Queensland Courts, offers a Juror Support Program. The program provides support for jurors once they have served in a trial, including free access to a medical practitioner, counsellor or psychologist.

The social and financial cost of psychologically damaged workers and jurors, who perform difficult work for the benefit of the community, cannot be quantified but should not be underestimated.

Although staff of the ODPP are not required to classify child exploitation material, clerks, legal officers and prosecutors are sometimes required to spend considerable time viewing this confronting material. Likewise for defence lawyers and support staff, whether engaged by Legal Aid or in private practise. The Work Health and Safety Act 2011 requires that the risk of harm to workers exposed to child exploitation material is eliminated, or at least reduced, so far as is reasonably practicable.

Recommendation

The Commission recommends that:

4.2 The Office of the Director of Public Prosecutions considers implementing guidelines similar to the Commonwealth Director of Public Prosecutions’ Online child exploitation conduct of matters guideline, particularly as it relates to limiting the time a member of staff is exposed to child exploitation material in any one sitting.

4.3 The Commission recommends that Legal Aid Queensland considers implementing guidelines similar to the Commonwealth Director of Public Prosecutions’ Online child exploitation conduct of matters guideline, particularly as it relates to limiting the time a member of staff is exposed to child exploitation material in any one sitting, for the protection of its officers (and preferred suppliers) who are exposed to child exploitation material.

(Endnotes)

1 Section 207A Criminal Code.
4 Transcript of Interview, Jon Rouse, 18 August 2015, pp. 20–21.
5 R v MJC (Unreported, District Court of Queensland, Koppenol DCJ, 23 November 2011).
7 R v STK (Unreported, District Court of Queensland, Dearden DCJ, 21 August 2013); Schedules of facts provided by the Queensland Office of the Director of Public Prosecutions in response to issued notice.
8 R v STK (Unreported, District Court of Queensland, Dearden DCJ, 21 August 2013).
9 Section 473.1 Criminal Code (Cth).
12 Crimes Legislation Amendment (Sexual Offences Against Children)
4.4 Related activities

The Terms of Reference focused the Commission’s attention on a number of ‘key enablers’. In the area of online child sex offending, including the child exploitation material market, three of the key enablers are particularly relevant:

- Cyber and technology-enabled crime
- Violence and extortion
- Professional facilitators—namely, IT experts and technical security experts

The child exploitation material market operates globally with an estimated 9,550 websites across 28 countries and 1,561 web domains being reported for child abuse material to the Internet Watch Foundation in 2012 alone. The Internet Watch Foundation is the UK hotline for reporting criminal online content. Its reported figures are likely to represent only the tip of the iceberg since child pornography exists in numerous domains—many located within hidden areas of the Internet or on private networks.

Many of those involved in the child exploitation material market, and those using the cyber environment to abuse children, are known to use whatever technology is available to achieve maximum anonymity and avoid detection.

4.4.1 Cyber and technology-enabled crime

Although referred to as an enabler or facilitator of online child sex offending (including the child exploitation material market), cyber and technology-enabled crime is an intrinsic part of the crime type itself. The proliferation of the market is made possible by technologies that usually have legitimate purposes, to hide offenders and their activities from authorities. The cyber environment also facilitates the formation of global networks of offenders who share their technical expertise with others in order to continue to operate under the radar.

The case studies outlined in this chapter above demonstrate that offenders in the child exploitation material market have infiltrated all parts of the Internet. Email and chat rooms are also commonly used for communication between offenders. For obvious reasons offenders are constantly seeking new and improved ways to achieve anonymity through the use of passwords, encryption and by taking advantage of the Darknet.

The Darknet has already been referred to in some detail, particularly as it relates to the facilitation of the drug trade. The Darknet is the term used to describe the anonymous networks within the deeper parts of the Deep Web. It is usually only accessible using programs such as Tor, I2P or Freenet since data is encrypted and users must be anonymous. Some of the content found on the Darknet is innocuous and arguably quite valuable. A large portion of it, however, contains questionable and illegal material, including child exploitation material along with services offering contract killings, and the sale of illegal drugs and weapons.

The iceberg analogy is an effective way of demonstrating the scale of the Deep Web. The open Internet (or Surface Web) is the part of the Internet most commonly used. As explained above, the Surface Web is readily accessible by a web browser and it is characterised by the ability to monitor communications and interactions between users. Search engines such as Google and Yahoo index sites on the Surface Web, allowing them to be found by users, and Internet Protocol (IP) addresses allow users activities to be traced.
The Deep Web is an umbrella term, which refers to any part of the Internet that traditional browsers such as Google, Chrome or Firefox will not search or index. Most of the content on the Deep Web is benign, whether it is hidden deliberately or is simply not indexed due to its unpopularity or web format. Company intranets and personal Hotmail inboxes are on the Deep Web since it is not appropriate that they be indexed and ‘searchable’ by the public. Large quantities of valuable information also exists on the Deep Web (for example, research, guides and independent new websites) and research is constantly being conducted by web companies to index these pages on their search engines.

Google is the most successful search engine and it currently indexes about eight billion web pages. That accounts for approximately four per cent of the Internet. The remaining content on the Internet exists on the Deep Web, protected by passwords and layers of encryption. The Darknet, and the child pornography sites it hides, is a part of the Deep Web.

**The Onion Router (Tor), I2P and Freenet**

Specialist browsers are required to access information on the Deep Web. The most commonly known specialist browser is The Onion Router (Tor), however alternatives such as I2P and Freenet are available. Unlike the Surface Web where websites can be accessed regardless of the search engine used, certain content is only available through certain browsers on the Deep Web. That is, if a site is configured for Tor it will not be accessible using I2P or Freenet.

As outlined earlier in this chapter, Tor was initially developed by the United States Naval Research Laboratory. Its ongoing development is overseen by the Tor Project. Tor allows communication and access to information without IP addresses leaving a digital footprint. It is described as a free browser that enables anonymous communication online.

The veil of anonymity comes from Tor’s use of onion routing. That process involves the encryption of data multiple times before sending it to randomly selected Tor relays. Each relay will decrypt only one layer of encryption to reveal the data’s next relay destination, with the final relay decrypting the inner most layer before sending the data to its destination without revealing (or even knowing) the source IP address. In the same way that a message becomes increasingly jumbled as it passes from person-to-person in a game of Chinese Whispers, data travelling through Tor relays are encrypted at every point, making tracing data packets to their original source incredibly difficult.
In order to access the Deep Web, you need to use a dedicated browser. Tor (The Onion Router) is the most commonly used, but other options such as I2P and Freenet offer an alternative solution.

When using the Surface Web, you access data directly from the source.

This direct approach tracks the information downloaded, from where and when it was accessed, and your exact location.

Information on the Deep Web cannot be accessed directly. This is because data is not held on any single page, but rather in databases, which makes it difficult for search engines to index.

Files are shared through any number of computers connected to the Internet that hold the information you need. This is known as peer-to-peer networking.

This method of sharing encrypted data makes it difficult for your location and the kind of information you access to be tracked or monitored.


I2P differs from Tor in that it uses ‘garlic routing’ rather than ‘onion routing’. Garlic routing differs by grouping multiple messages, making it increasingly difficult to conduct Internet traffic analysis. 3
I2P is primarily used as an anonymous peer-to-peer network allowing users to share information directly between them. I2P users are able to configure the program to enter ‘Dark Mode’, which establishes a secure, anonymous connection between trusted computers similar to more traditional peer-to-peer (P2P) networks. Considering that I2P aims to isolate users within the Internet, allowing them to share material exclusively between other anonymous users, it has been identified as a platform harbouring significant quantities of child exploitation material. The networks of offenders are, however, probably looser than those seen to be operating on Tor.

Freenet has also become notorious for hosting mass quantities of child exploitation material. Whereas I2P sites (known as Eepsites) exist on only one computer, Freenet’s sites (Freesites) float around the Freenet network between users in a decentralized manner. Many have argued that this feature makes the Freenet more secure than I2P.

Encryption and passwords

Most people are very familiar with the concept of password protection. It is the most common method of data protection, and the threat of data and identity theft (discussed in detail in the chapter on financial crimes) has led to a need for the public to be vigilant in taking security precautions. The public are being actively and regularly encouraged to ensure that passwords are more complex and therefore less susceptible to breaches.

Encryption is the process of encoding messages or information so that only authorised parties can decipher it. It converts ‘plain text’ to ‘cipher text’, and while that does not prevent interception of the information, it denies the interceptor access to the content. A decryption key (or password) held by an authorised interceptor will easily decrypt the information.

Encryption can be used to protect data ‘at rest’, such as collections of child exploitation material stored on computers and USB flash drives. Data can also be protected while ‘in transit’ via networks, mobile phones, wireless microphones, wireless intercom systems, Bluetooth devices and automatic teller machines. While it is well known that many encryption systems have weaknesses, and it is certainly possible to access encrypted data without the key, specialist resources are usually required.

Encryption has long been used by the military and governments to protect secret information and communications. It is now commonly used as a legitimate tool for law-abiding organisations and individuals to protect their data. There are countless websites and forums offering advice about the myriad of encryption tools available. Many such tools are free to download.
It is unsurprising that online child sex offenders, particularly those involved in the child exploitation material market, often use encryption to protect their communications and material from the eyes of others, especially law enforcement officers.

**Hacking and the use of virtual currencies**

Research by the Internet Watch Foundation in 2014 led to the discovery of a ‘current and emerging trend’ involving the hacking of legitimate websites which then become unwitting hosts for child exploitation material. The sites used were found to be diverse in content and location (in North America and EU countries) but were mostly hosted by small businesses and voluntary organisations.

The author of the IFW report opined that ‘the most likely explanation for these sites being hacked is that they have poor website security and are therefore vulnerable to compromise.’ It follows, as a matter of common sense, that it is of critical importance for businesses and individuals to employ basic security measures for their websites and servers to prevent compromise.

The Internet Watch Foundation found that a ‘previously unobserved top level commercial distributor’ was using hacked websites to provide access to child abuse material. It was the first time the Foundation had seen Bitcoin (a digital currency) purported as the only method of payment for child abuse material available on the Surface Web, as opposed to material hidden on the Darknet.

The discovery was said to be significant, because that payment method had not previously been associated with payment for child abuse material, and it confirmed long-held concerns by law enforcement and experts in the field that it was only a matter of time. As at July 2014, IFW had identified 22 websites hacked with commercial templates exclusively accepting Bitcoin as payment for material.

Virtual currencies, particularly Bitcoin, are discussed in detail in the section on the Internet and drugs, above. The Australian Crime Commission, through Project Longstrike, is now monitoring Bitcoin-enabled crime, having spent considerable time building technologies capable of tracking transactions.

Project Longstrike is part of the ‘Making Australia Hostile to Organised Crime’ initiative and aims ‘to develop an enhanced understanding of the national and international environment in the detected misuse of virtual currencies to facilitate criminal activity.’ Such criminal activity includes that which makes use of Darknets ‘to harbor trading in illicit commodities, including child exploitation material, (as well as) illicit drugs and firearms, stolen credit card and identity data, and hacking techniques.’

Further, in October 2014, the Australian Senate referred the matter of digital currency to the Economics References Committee for inquiry. The purpose of the inquiry was to ‘examine how best to define digital currency within the regulatory frameworks in order to support innovation and the need of the growing Australian digital currency industry.’ The Committee reported in August 2015.

The Committee examined the risks and benefits of virtual currencies. No mention is made in the report of the use of such currencies to purchase child exploitation material, probably because examples at present are few. However, the submission of the Attorney-General’s Department did note that:

> Digital currencies provide a powerful new tool for criminals, terrorist financiers and sanctions evaders to both move and store illicit funds out of the reach of law enforcement and other authorities and purchase illicit good and services.

Information received from the Australian Federal Police by the Committee suggested that while digital currencies were not currently ‘a significant operational issue’, there was that potential for the future. Given that the digital currency industry is still in its early stages ‘the committee supports a “wait-and-see” approach.
to government regulation.' It recommends close monitoring by relevant government agencies and the establishment of a Digital Economy Taskforce to gather further information on the uses, opportunities and risks associated with digital currencies.

4.4.2 Violence and extortion

'Sextortion', or sexual exploitation through extortion, has been described as a new ‘industrial-scale’ crime.13 It has been defined by a special agent with the Federal Bureau of Investigation in the United States as occurring when a person threatens to distribute private and sensitive material unless they are provided with images of a sexual nature, sexual favours or money.14

There are many examples of lone offenders, some having ‘sextorted’ large numbers of young men and women. There have also been disturbing instances of huge rings of offenders exploiting children for profit by threatening to send sexually explicit material to their friends and family.

One global syndicate, operated out of the Philippines, was described as ‘massive’. An international operation coordinated by Interpol led to the identification of between 190 and 195 individuals working for organised crime groups connected with the syndicate, and resulted in 58 arrests. Victims were traced to numerous countries through close cooperation between law enforcement agencies. Potential victims were identified in Australia and one Scottish victim is known to have committed suicide as a result of what happened to him. That young man, 17 years old, was enticed to send explicit photos of himself to a person he thought was a teenage girl. He was then blackmailed by the offender who demanded money lest the images be posted on social networking sites.

Interpol describes call centre-style offices staffed by cyber-blackmail agents who are provided with training and offered bonus incentives such as holidays, cash or mobile phones for reaching financial targets.15

Another modus operandi of large-scale sexual extortion involves a combination of web cam scamming and blackmail, and exploits people on dating web sites, in chat rooms and on social networking platforms. Once offenders make contact with a victim, contact is moved to web cam contact where the victim can be secretly filmed engaging in sexual activity. The victims are then blackmailed to prevent the videos being distributed.

The case study of R v Tahiraj above, while an example of a lone offender, demonstrates another alarming technique used by offenders to engage in ‘sextortion’: using malware to access a victim’s web cam remotely.

There is no doubt that the success of ‘sextortionists’, operating alone and in organised crime groups, depends on the willingness of young people to share explicit material and on weaknesses in systems security. Education campaigns promoting more guarded online conduct and the need for security measures on devices are paramount. As recently observed by the European Financial Coalition against Commercial Sexual Exploitation of Children Online:

Sharing sexualized content online seems to be a part of adolescent development and of the sexual exploration process of young people who nowadays have become members of a digital society by default. Materials originally produced for private consumption now end up in unwanted circulation and happen to attract the attention of people with a sexual interest in children, or profit oriented individuals who may use them as part of grooming or threatening processes.

Awareness campaigns should not be limited to minors only. Parents also need to be aware of the existence of social network profiles such as ‘The most sexy 4, 5, 6 years old’. These profiles can access and use photos of people’s offspring from their own profile for less than innocent purposes. Such opportunism on the part of those operating those profiles emphatically proves that there is a great need to educate, not only children, but also their parents.16

While it was beyond the scope of this Inquiry to ascertain the scope and impact of cyber safety education provided to Queensland children, a review of information available online, on websites for agencies and departments such as the Australian Curriculum, the Australian Government Department of Communications, the Office of the Children’s eSafety Commissioner and the Queensland Government and QPS, indicate that there is a plethora of material available to help carers and teachers instil the cyber safety message.
4.4.3 IT experts and technical security experts

There is no doubt that IT experts and technical security experts enable child sex offending, particularly in the child exploitation material market. Such experts facilitate organised crime in this area by developing and administering sites such as that which was administered by Shannon McCoole. Experts offered advice to members of that site regarding security and anonymity. That kind of technical support is often provided in child exploitation material forums, allowing lower-level offenders to become experts themselves.

The ICT industry is completely unregulated, and it is unlikely that attempts at regulation would have any impact on the child exploitation material market. That is due to the increasing level of technical expertise of people who do not belong to the industry through the attainment of formal qualifications, membership or employment.

There is no minimum education or certification requirement for an individual to be employed as an ICT professional. Data from July 2013 indicates that 50 to 77 per cent of workers in ICT occupations hold a higher education qualification; however, recruitment of ICT workers is often achieved through non-traditional channels and in ways that assess capabilities rather than formal qualifications.17

Membership of a professional industry body is not compulsory for those considered ICT professionals. Professional bodies do exist, but usually for the primary purposes of advocating the interests of their members and providing networking opportunities. The Commission identified two relevant membership bodies in Queensland:

- The Australian Computer Society (ACS)
- IT Queensland

The ACS is the professional association for the ICT sector in Australia. It represents approximately 22,000 practitioners in the business, government and education sectors. The ACS provides a certification process that enables its members to advertise themselves as possessing specialist expertise as either a ‘Certified Technologist’ or a ‘Certified Professional’.

Members are held to account by the ACS Code of Professional Conduct and a Code of Ethics. Compliance with those codes is a requirement of membership. In addition to acting within the law, members are required to conduct themselves with six principles in mind:

- the primacy of the public interest
- the enhancement of quality of life
- honesty
- competence
- professional development
- professionalism

The ACS informed the Commission that it has a complaints procedure, and that in the period since January 2012 (the period nominated by the Commission as being relevant to the Inquiry), it has not become aware of any of its members facilitating the distribution of child exploitation material.18 The Commission was informed that although the ACS does not have any formal policies or procedures dealing with cooperation with law enforcement, it would cooperate in the event it was asked to provide assistance/information in respect of an investigation involving online child sex offending.

IT Queensland was established in 2004. It is essentially a peer-led organisation which aims to assist business development for its members. It also hopes to raise the ICT industry profile within the general community and lobby government to address issues of concern to its membership. Like the ACS, membership is voluntary.

IT Queensland is not aware of any instance involving the use of the Internet or electronic technology by a member for the purpose of facilitating the distribution of child exploitation material. It does not have a
code of conduct, a complaints procedure or a procedure dealing with cooperation with law enforcement authorities. IT Queensland did, however, inform the Commission that it would cooperate with authorities if required.19

The Commission inquired of the Crime and Corruption Commission and the QPS as to the number of known IT experts and/or technical security experts that have been directly or indirectly involved in the commission or facilitation of Internet, electronic, or technology-enabled child sexual offending, including in the child exploitation material market, over the past three years. Surprisingly few names appeared in the responses received.20

Despite a lack evidence in the form of successful prosecutions, as to the involvement of IT experts and technical security experts as professional facilitators in this area, the research of the Commission, combined with the clear message from those involved in policing online child sex offending, is that those involved in the market are increasingly skilled.

Sophisticated sites with measures to avoid detection are being developed and maintained by people who have clear expertise in Information and Communications Technology. Even users who might not be considered experts are, however, operating with a level of technical aptitude that continues to pose challenges for law enforcement agencies.

(Endnotes)


2 Egan, M. (2015). What is the Dark Web? How to access the Dark Web – How to turn out the lights and access the Dark Web (and why you might want to). Available at www.pcadviser.co.uk.

3 Gallagher, S. (2015). Under the hood of I2P, the Tor alternative that reloaded Silk Road. Available at http://arstechnia.com


15 European Financial Coalition against Commercial Sexual Exploitation of
4.5 Legislation

4.5.1 Legislative framework

This chapter has already made reference to the offences created, and maximum penalties imposed, by the Commonwealth and Queensland Criminal Codes for online child sex offending and offences involving participation in the child exploitation material market.

The Commission considers that the legislative framework created by those statutes, for the most part, adequately deals with the gamut of offending in the area of online child sex offending, including the child exploitation material market. Importantly, the amendments to the Criminal Code (Cth) in 2013 mean that there is now an aggravated offence recognising networked offending, as well as provisions dealing with extraterritorial conduct involving the abuse of children and participation in the global child exploitation material market.

However, a gap in the framework exists in respect of administrators of child exploitation websites, where dealing in the child exploitation material cannot be proved, and in respect of those who encourage others to engage in the child exploitation material market and those who provide advice on avoiding detection by law enforcement agencies.

It is also concerning is that there is an absence of disincentives to offending within the anonymity of the Darknet (using Tor for example), and too little disincentive to refuse to cooperate with authorities by disclosing passwords and keys for encrypted data. In addition, law enforcement officers expressed concerns to the Commission regarding requirements for Internet Service Providers (ISPs) to retain data necessary for their investigations.

Insofar as the prosecution and sentencing offenders in this area is concerned, the Commission was also made aware of issues relating to the classification of child exploitation material files. Both the Queensland Police Service (QPS) and Crime and Corruption Commission (CCC) suggest a streamlining of the classification system to increase efficiency. Officers from both agencies expressed strong opposition to the continued use of the Oliver scale in sentencing child exploitation material offenders. The Office of the Director of Public Prosecutions (ODPP) also identified the process of classifying vast quantities of material as contributing to some delays in prosecuting offenders. It is recommended below that this issue be prioritised by the Queensland Government’s proposed new Sentencing Advisory Council.

Those gaps and inadequacies are dealt with below in the following way –

- **Child exploitation material and offending in the Darknet**: recommends additional offences to criminalise administrators of child exploitation material sites and those who encourage participation in the child exploitation material market and provide advice about avoiding detection, increased penalties for offenders involving a child in and making child exploitation material, a circumstance of
aggravation for offenders using the Darknet and other anonymising services to engage in the child exploitation material market.

- **Sexual servitude and deceptive conduct**: looks at the provisions enacted in other jurisdictions and addresses the adequacy of the Queensland statute.

- **Access to stored information**: addresses the current police power to compel an offender to provide access to stored information (including child exploitation material) and the consequence for non-compliance, as well as the requirements for ISP to retain data.

- **Blocking child exploitation material**: explores the methods that are currently used to block content, and the possibility of doing more to prevent access to offending websites and files.

- **Classification**: deals with an issue raised by various agencies in respect of the time-consuming classification of collections of child exploitation material using the existing so-called ‘Oliver scale’.

### 4.5.2 Legislative gaps or inadequacies

**Child exploitation material and offending in the Darknet**

The range of offences detailed in the section titled Online child sex offending deal with offenders who use the Internet, incorporating the Surface Web and Deep Web, to participate in the child exploitation material market. The maximum penalty is 14 years imprisonment for possessing, making, and involving a child in making child exploitation material, and for distribution of child exploitation material. The maximum penalties were increased by the *Criminal Law (Child Exploitation and Dangerous Drugs) Amendment Act 2013* from five years (for possessing child exploitation material) and 10 years (for making and distributing child exploitation material).

The amending Act also introduced the offence of ‘grooming’ under section 218B and increased the maximum penalty for the offence of using the Internet to procure children under 16 to engage in a sexual act (Section 218A) from five years to ten years imprisonment. The existing circumstance of aggravation applying to offending against a child under 12 years now carries a maximum penalty of 14 years (increased from 10 years) and a new circumstances of aggravation was created to deal with procuring conduct which involved the offender meeting the child or travelling with the intention of meeting the child.

The increase in the maximum penalties for child exploitation material offences was said to reflect the seriousness of the offences and to align with the penalties for comparable Commonwealth offences. In acknowledging the removal of any distinction between the different types of conduct (for example, possession versus distribution), the Explanatory Memorandum states:

> While the criminal law generally regards the distribution of contraband as objectively more serious than mere possession, the commodity in question in the case of child exploitation material offences is a child who is the subject of appalling physical and sexual abuse. The market for such material must be targeted. This approach is consistent with the way in which the offence of receiving tainted property is dealt with under the Criminal Code. Receiving tainted property creates a market for criminal activity such as theft. In recognition of this factor, a higher maximum penalty is applied to the offence.

Removing the current penalty distinction also recognises the wide variety of circumstances in which child exploitation material offences can be committed and that there will be cases where the mere possession of material carries a greater criminality that the offence of distributing. For example, a person may possess hundreds of thousands of depraved images, depicting the penetration and torture of infants and toddlers; as opposed to a person who forwards an animated image depicting a child in a sexually explicit pose.
Commonwealth offences do not make the distinction in relation to these types of offences with all carrying a maximum penalty of 15 years imprisonment. In New South Wales and the Northern Territory, the offences of possession, production and distribution all carry a maximum penalty of 10 years imprisonment.

The Commonwealth Criminal Code, as already mentioned, also contains an aggravated offence which applies when a person commits one of the relevant offences (involving the use of a carriage service for child pornography or child abuse material, and possessing, controlling, producing, supplying or obtaining such material for use through a carriage service) on three or more occasions, and the commission of the offences involved two or more persons. That offence has been referred to in this report as the ‘networking offence’. It carries a maximum penalty of 25 years imprisonment.

While addressing the networked nature of online child exploitation material offenders, the Commonwealth aggravated offence would not necessarily capture administrators of child exploitation material websites where it cannot also be proved that those administrators committed one or more of the relevant offences, on three occasions, involving two or more persons.

By way of example, in the case involving Shannon McCoole, the aggravated offence was charged based on his involvement as head administrator of a highly organised child exploitation material website, and on evidence of his using a carriage service to transmit child exploitation material on more than three occasions to two or more people. However, there were seven co-administrators below McCoole in the ‘management’ hierarchy against whom the aggravated offence might not be available because of the need to prove that those people dealt with child exploitation material in one or more of the proscribed ways on the requisite number of occasions. That is, there might be circumstances in which it can be proved that a person was engaged in supporting a website as an administrator, but not that the person has otherwise dealt with the child exploitation material content. In that case, as far as the Commonwealth legislation is concerned, there is potentially no supportable criminal offence.

Further, those people who encourage others to use a website such as that operated by Shannon McCoole, and those who provide advice on avoiding detection by law enforcement agencies, without proof of an offence committed as a result, are not necessarily caught by existing legislation.

**New offences for website administrators, people who encourage their use and provide information to avoid detection**

In Queensland, an administrator of such a website might be charged as a ‘party’ to one or more of the child exploitation material offences (for possessing, making or distributing child exploitation material) under section 7 (for enabling or aiding the commission of an offence) or section 8 (for acting in the prosecution of a common unlawful purpose to commit an offence) of the Criminal Code. Likewise, a person who counsels or procures the commission of an offence (for example, by encouraging a person to possess, make or distribute child exploitation material), is guilty of an offence as a party under section 7 (d) of the Criminal Code. Section 9 is also relevant to offenders who are alleged to have counselled the commission of an offence, such as distributing child exploitation material.

Section 7 of the Criminal Code provides:

1. When an offence is committed, each of the following persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say –
   a. every person who actually does the act or makes the omission which constitutes the offence;
   b. every person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence;
   c. every person who aids another person in committing the offence;
   d. any person who counsels or procures any other person to commit the offence.
(2) Under subsection (1)(d) the person may be charged either with committing the offence or with counselling or procuring its commission.

(3) A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence.

(4) Any person who procures another to do or omit to do any act of such a nature that, if the person had done the act or made the omission, the act or omission would have constituted an offence on the person’s part, is guilty of an offence of the same kind and is liable to the same punishment, as if the person had done the act or made the omission; and the person may be charged with doing the act or making the omission.

Section 8 of the Criminal Code provides –

When 2 or more persons form a common intention to prosecute an unlawful purpose in conjunction with one another, and in the prosecution of such purpose an offence is committed of such a nature that its commission was a probably consequence of the prosecution of such a purpose, each of them is deemed to have committed an offence.

Section 9 of the Criminal Code provides –

(1) When a person counsels another to commit an offence, and an offence is actually committed after such counsel by the person to whom it is given, it is immaterial whether the offence actually committed is the same as that counselled or a different one, or whether the offence is committed in the way counselled, or in a different way, provided in either case that the facts constituting the offence actually committed are a probable consequence of carrying out the counsel.

(2) In either case the person who gave the counsel is deemed to have counselled the other person to commit the offence actually committed by the other person.

There are limitations on the use of sections 7 and 8 of the Criminal Code to prosecute those who administer child exploitation material websites, encourage participation in them or who counsel others to avoid detection.

Firstly, proof of the commission of an offence is required before liability as a party to it can be established. One of the difficulties faced where a website is administered in the anonymous environment of the Darknet, with users from indeterminate locations all over the world, is that it might not be possible to draw the causal link between the acts of the administrator (or the encourager, or the person providing instructions to avoid detection) and the commission of an offence by another person. Provisions recently enacted in Victoria overcome that difficulty.

Secondly, the jurisdictional nexus to allow prosecution in Queensland required by sections 12, 13 and 14 of the Criminal Code means that, for example, an administrator based outside Queensland could not be prosecuted for facilitating participation in the child exploitation material market unless:

- part of the offence was committed in Queensland (section 12); or
- an offence committed in Queensland was enabled, aided, counselled or procured by the person while outside Queensland (section 13); or
- an offence was procured by the person while in Queensland (section 14).

Those provisions would preclude the prosecution of an overseas-based website administrator where proof of the commission of an offence, or part of an offence, in Queensland is impossible and no offence was procured by that person while in Queensland. The new Victorian provisions deal with circumstances where it can at least be proved that a person (even of unknown identity) dealt with (including by viewing) offending material in Victoria.

The Crimes Amendment (Child Pornography and Other Matters) Act 2015 (Vic) received Royal Assent on 22 September 2015. The Act contains three new offences that will be inserted into the Crimes Act 1958 (Vic)
and "make it easier to prosecute online-related activities that facilitate the commission of child pornography offences, and ensure that offenders can be prosecuted for their crimes."2

The first offence targets administrators of child pornography websites, including those who create the sites, regulate membership and monitor traffic on such sites. A defence applies if an administrator becomes aware that their website is being used for child pornography and takes all reasonable steps to prevent access to the pornography.3

Section 70AAAB (Administering a child pornography website), to be inserted into the Crimes Act 1958 (Vic), provides –

(1) A person (A) commits an offence if –
   (a) A administers, or assists in the administration of, a website; and
   (b) the website is used by another person to deal with child pornography; and
   (c) A –
      (i) intends that the website be used by another person to deal with child pornography; or
      (ii) is aware that the website is being used by another person to deal with child pornography.

Examples
1. A manages membership of a website. A intends that the website be used by other persons to view child pornography.
2. A monitors traffic through a website and ensures that the web server hardware and software are running correctly. A is aware that the website is being used by other persons to download child pornography.

(2) A person who commits an offence against subsection (1) is liable to level 5 imprisonment (10 years maximum).

(3) It is not necessary to prove the identity of the person using the website to deal with child pornography.

(4) A person is not guilty of an offence against subsection (1) if the person, on becoming aware that the website is being used, or has been used, by another person to deal with child pornography takes all reasonable steps in the circumstances to prevent any person from being able to use the website to deal with child pornography.

(5) In determining whether a person has taken all reasonable steps in the circumstances to prevent any person from being able to use a website to deal with child pornography, regard must be had to whether the person did any of the following as soon as it was practicable to do so—
   (a) notified a police officer that the website is being, or has been, used to deal with child pornography and complied with any reasonable directions given to the person by a police officer as to what to do in relation to that use of the website;
   (b) notified a relevant industry regulatory authority that the website is being, or has been, used to deal with child pornography and complied with any reasonable directions given to the person by that authority as to what to do in relation to that use of the website;
   (c) shut the website down;
   (d) modified the operation of the website so that it could not be used to deal with child pornography.

(6) Subsection (1) does not apply to conduct engaged in by a person in good faith—
   (a) in the course of official duties of the person—
(iii) connected with the administration of the criminal justice system including the investigation or prosecution of offences; or

(iv) as an employee of the Department of Justice and Regulation who is authorised to engage in that conduct by the Secretary to that Department; or

(b) for a genuine medical, scientific or educational purpose.

(7) Subsection (1) does not apply to any dealing with a film, publication or computer game that, at the time of being dealt with, was classified other than RC or would, if classified, have been classified other than RC.

(8) It is immaterial that some or all of the conduct constituting an offence against subsection (1) occurred outside Victoria or that a computer or device used in connection with administering the website was outside Victoria, so long as—

(a) the person using the website to deal with child pornography was in Victoria; or

(b) the computer or device used to deal with child pornography was in Victoria.

(9) It is immaterial that the person using the website to deal with child pornography was outside Victoria or that the computer or device used to deal with child pornography was outside Victoria, so long as—

(a) some or all of the conduct constituting an offence against subsection (1) occurred in Victoria; or

(b) a computer or device used in connection with administering the website was in Victoria.

To ‘deal’ with child pornography, includes:

(a) viewing, uploading or downloading child pornography;

(b) making child pornography available for viewing, uploading or downloading;

(c) facilitating the viewing, uploading or downloading of child pornography

The definition of ‘child pornography’ in section 67A of the Crimes Act 1958 (Vic) is more narrow than the definition of ‘child exploitation material’ in the Criminal Code (Qld). It means ‘a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor (under 18 years) engaging in sexual activity or depicted in an indecent sexual manner or context.’

The offence of administering in section 70AAAB, and its defence, will presumably have the additional benefit of deterring legitimate operators from turning a ‘blind-eye’ to offending material within their control. Administrators of websites who know that the site hosts child pornography are guilty of the offence unless all reasonable steps in the circumstances are taken to prevent any person from being able to use the website to deal with child pornography.

Significantly, for proof of the offence against an alleged administrator, it is not necessary to prove the identity of the person(s) who uses the website to deal with child pornography. It is sufficient to prove that an unidentified person has viewed offending material on the website. That lowers the bar set by sections 7 and 8 of the Criminal Code (and the Victorian ‘complicity provisions’) which require proof of the commission of an offence.

Further, the jurisdictional provisions in subsections (8) and (9) mean that an overseas-based administrator, or an administrator using a computer or device located outside the jurisdiction, is guilty of the offence if a person using the website to deal with child pornography is located in Victoria. In the corollary, if the person using the website to deal with child pornography is located outside Victoria, it is sufficient that the administrator engaged in some of the conduct proscribed by subsection (1) in Victoria, or if the computer or device used in connection with administration of the website was in Victoria.
The second offence will criminalise conduct that encourages others to use a website to deal with child pornography, for example by promoting or advertising a website. It will not be necessary to prove that a person was actually encouraged by the person, but that the person encouraged another with the intention that the other will use a child pornography website. That type of offending would not be caught by existing Queensland legislation which requires (by virtue of section 7 of the Criminal Code) that the encouragement lead to the commission of an offence.

Section 70AAAC (Encouraging use of a website to deal with child pornography) provides:

(1) A person (A) commits an offence if –
   (a) A is 18 years of age or more: and
   (b) A encourages another person to use a website; and
   (c) A intends that the other person use the website to deal with child pornography.

(2) A person who commits an offence against subsection (1) is liable to level 5 imprisonment (10 years maximum).

(3) In determining whether A has encouraged another person to use a website to deal with child pornography, it is not necessary to prove –
   (a) the identity of the person encouraged to use the website to deal with child pornography; or
   (b) that another person in fact used the website to deal with child pornography; or
   (c) if another person did in fact use the website to deal with child pornography, that it was A’s encouragement that caused the person to do so.

(4) Despite anything to the contrary in Division 12 of Part 1, it is not an offence for a person to attempt to commit an offence against subsection (1).

(5) It is immaterial that some or all of the conduct constituting an offence against subsection (1) occurred outside Victoria, so long as the person being encouraged was in Victoria at the time at which the conduct occurred.

(6) It is immaterial that the person being encouraged was outside Victoria at the time the conduct constituting an offence against subsection (1) occurred, so long as that conduct occurred in Victoria.

Note: If an adult uses a minor as an innocent agent to encourage another person to use a website, intending that the other person use the website to deal with child pornography, the adult commits an offence against subsection (1).

The third offence targets those who provide information to another person about ways to evade apprehension for a child pornography offence. The offence might apply to a person who provides advice to others about how to use a website anonymously, or about how to encrypt files containing child pornography. That type of conduct was seen on the website administered by Shannon McCoole, and on other sites seen by Taskforce Argos.

Section 70AAAD (Assisting a person to avoid apprehension) provides:

(1) A person (A) commits an offence if –
   (a) A intentionally provides information to another person (B); and
   (b) A intends that B use the information for the purpose of avoiding or reducing the likelihood of apprehension for an offence committed by B against –
      (i) Section 68 (production of child pornography), 69 (procurement etc. of a minor for child pornography), 70 (possession of child pornography), 70AAAB or 70AAAC; or
      (ii) Section 57A (publication or transmission of child pornography) of the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995.
Examples:

1. A provides information to B about how to use a website to deal with child pornography anonymously or how to encrypt files containing child pornography.
2. A provides information to B about how to delete electronic data that records information about B’s identity.

(2) A person who commits an offence against subsection (1) is liable to level 5 imprisonment (10 years maximum).

(3) It is not necessary to prove –
   (a) the identity of the person to whom the information was provided; or
   (b) that the information was actually used by the other person.

(4) It is immaterial that some or all of the conduct constituting an offence against subsection (1) occurred outside Victoria, so long as the other person was in Victoria at the time at which the conduct occurred.

(5) It is immaterial that the other person was outside Victoria at the time the conduct constituting an offence against subsection (1) occurred, so long as that conduct occurred in Victoria.

(6) For the purposes of subsections (4) and (5), information is provided by A to B at the place where A is at the time of giving that information irrespective of where B is at the time of receiving that information.

The three offences carry the same maximum penalty as for the offence of producing child pornography, which, in Victoria, is 10 years imprisonment. Importantly, they fill a gap in the legislative framework and deal with offending conduct that seems to be becoming more prevalent. The offences aim to deter and punish facilitators in the child exploitation material market, those who encourage participation in it and those who act to make the job of law enforcement more difficult. Removing any need to prove the identity of participants in the market, or proof of participation beyond a person having dealt with the material, also addresses the reality of this type of global offending in the anonymous environment of the Darknet.

Recommendation

4.4 The Commission recommends that the Queensland Government amend the Criminal Code to include provisions that would criminalise the contribution of administrators of child exploitation websites, as well as those who encourage their use and provide advice to avoid detection and add to the proliferation of child exploitation material online. In developing the new provisions regard should be had to sections 70AAAB, 70AAAC and 70AAAD of the Crimes Act 1958 (Vic).

Increase in maximum penalties for making child exploitation material and a proposed circumstance of aggravation

A further concern shared by Taskforce Argos officers and officers attached to the CCC Cerberus Investigation Unit (Cerberus) is that the use of the Darknet, as well as other proxies and anonymising services, makes detection and investigation of child exploitation material offenders much more difficult. Further, the nature of offending being committed within these hidden networks is generally more serious and more likely fall into the category of organised crime. The case of Shannon McCoole and other members of that Tor website provide stark examples.

In a presentation given to the Commission by officers from Taskforce Argos, those two serious aspects of child exploitation material offending in the Darknet were emphasised. The demonstration of a particular child exploitation material site operated on Tor, and of child exploitation material being shared on peer-to-peer
networks, highlighted for the Commission that the more sophisticated offenders in the child exploitation material market are operating in the Darknet, using sites that are organised and hierarchical (although to varying degrees).

It has already been mentioned that Darknet child exploitation material sites often require members to produce and/or distribute new material, and some offer on-demand abuse of children. Offending in that hidden part of the Internet is usually objectively more serious in nature, and much more difficult to detect, than offending using peer-to-peer networks (even using friend-to-friend encrypted networks) and other platforms on the Surface Web.

In order to provide a real deterrent to users of the Darknet and other anonymising services for illicit activity, particularly to commit online child sex offences, including child exploitation material offences, the Commission considers that higher penalties are called for in the case of offenders who engage in the child exploitation material market using the Darknet, or other anonymising service (including proxies).

The addition of a circumstance of aggravation would reflect the serious criminality involved in accessing an encrypted network which is known to promote anonymous features, rally against law enforcement measures and arguably contain more hard core, so-called ‘hurt core’, and highly sought-after images of child victims.

In considering the maximum penalties that might attach to such a circumstance of aggravation, the Commission also considered the adequacy of existing maximum penalties for offences under sections 228A (involving a child in making child exploitation material), 228B (making child exploitation material), 228C (distribution of child exploitation material) and 228D (possession of child exploitation material) of the Criminal Code. Each offence currently carries a maximum penalty of 14 years imprisonment.

Those offence provisions were introduced in 2005 to replace the existing legislative scheme under the Classification of Computer Games and Images Act 1995. Relevantly, that Act proscribed:

- possession of an objectionable computer game to sell or demonstrate in public, and knowing possession of a child abuse computer game – section 26
- making, or attempting to make, and production and copying, an objectionable computer game (for gain) or a child abuse computer game – section 27
- obtaining, or attempting to obtain a minor to be in any way concerned in the making or production of an objectionable computer game – section 28.

The maximum penalties ranged from two years (for possession of a child abuse computer game) to five years imprisonment (for making or producing a child abuse computer game).

An ‘objectionable computer game’ was defined as ‘a computer game, or an advertisement for a computer game, that (amongst other things not relevant for present purposes) –

(a) describes, depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence, or revolting or abhorrent phenomena, in a way that offends against standards of morality, decency and propriety generally accepted by reasonable adults; or

(b) depicts a person who is, or who looks like, a child under 16 years (whether the person is engaged in sexual activity or not) in a way likely to cause offence to a reasonable adult’

A ‘child abuse computer game’ was defined as ‘a computer game that is an objectionable computer game because it depicts a person who is, or who looks like, a child under 16 years (whether the person is engaged in sexual activity or not) in any way likely to cause offence to a reasonable adult.’

A ‘computer game’ relevantly included -

(a) a computer program and associated data, capable of generating a display of a computer monitor, television screen, liquid crystal display or similar medium; or

(b) a computer generated image; or

(c) an interactive film
The objective of the 2005 amendments was to recognise the ‘serious criminal and exploitative nature’ of child pornography offending by creating specific offences, with appropriate penalties, dealing with involving a child in, and making, distributing and possessing the newly defined ‘child exploitation material’. The amendments came in response to a recent national crackdown on an Internet child pornography ring resulting in hundreds of arrests across Australia which had raised the profile of existing state and interstate legislative provisions. It was recognised that ongoing discussion about the adequacy of existing offences and investigative powers might mean ‘further legislative amendment in due course.’

The new sections 228A, 228B, 228C and 228D updated the language used, moving to the reference to ‘child exploitation material’ rather than to ‘computer games’ along with the convoluted and outdated definitions that had been applied to try to deal with material that were not games of any kind. However, the new provisions reflected the conduct proscribed under the old regime including involving a minor in the production of material, making and producing material, and knowing possession of it. The new section 228D added distribution to the proscribed conduct.

The new sections were not intended to derogate from the liability of an offender for a more substantive offence relating to the activity in appropriate cases. For example, a person who took indecent photographs of a 10-year-old child would be liable to prosecution pursuant to section 210(1)(f) (taking an indecent photograph of a child under 16 years, and under 12 years). That offence carries a maximum penalty of 20 years imprisonment. If a person procured the rape of a child overseas while ‘directing’ a live-streamed video, that person would be exposed to a maximum penalty of life imprisonment for the offence of rape (combined with the extended jurisdiction provision in section 14 of the Criminal Code), provided there was sufficient evidence to prove that substantive charge. In both cases, the person could also be charged with making child exploitation material under section 228B of the Code.

In 2013, the maximum penalties for all child exploitation material offences were increased from five years imprisonment for section 228D (possession), and 10 years imprisonment for sections 228A, 228B and 228C (involving a child, making and distributing child exploitation material) to 14 years imprisonment for all offences. The reason for the increase in penalties was to recognise that child exploitation material offences are not victimless crimes, and that ‘children who are used in the production of exploitative material are often terribly abused and suffer severe trauma as a result.’ The Explanatory Memorandum further noted that ‘those who seek to possess such material feed this exploitative market.’

The rationale for imposing the same maximum penalty for all offences (whereas there had previously been a distinction between the ‘mere’ possession of material, and involving a child in, making and distributing material) was explained in the Explanatory Memorandum, as outlined above.

There is no doubt that all types of participation in the child exploitation material market is to be strongly denounced, and there are conceivable circumstances where the possession of material might represent greater criminality, and therefore attract a higher penalty than, for example, distribution. That does not, however, render otiose a distinction between possession and distribution of child exploitation material, and conduct that involves making new material now that it is known that the market is becoming increasingly depraved and voracious for new material, including pay-on-demand live-streaming services.

The Commission undertook an analysis of recent decisions of the District Court of Queensland and the Court of Appeal dealing with all types of offending in the child exploitation material market. That analysis demonstrated that courts are taking into account relevant sentencing principles and aggravating/mitigating features in order to arrive at appropriate sentences. For example, in R v Carr the defendant was sentenced to a term of actual imprisonment (six months) for possessing 22,000 images over an eight-month period where 700 images were in the worst categories; whereas in R v Amarandos a case involving distribution and possession of child exploitation material, a probation order was made to recognise various mitigating factors including youth and medical conditions.

For making child exploitation material, penalties vary widely depending on the level of exploitation of the child(ren) and the personal circumstances of the offenders. The case studies below provide examples of this:
Case study

R v Musgrove

The defendant pleaded guilty to one count of making child exploitation material and one count of possessing child exploitation material.

The defendant took photographs and videos of possibly up to nine girls, ranging in age from small children to teenagers. The images depicted the groin area of the children. The children were photographed at the beach or in a playground. The defendant secretly manipulated the camera to take photographs of the girls’ bottoms or crotches. On some occasions, the defendant filmed from a distance but on other occasions, he directed the children where to sit or how to place their legs, engaging them in friendly conversation. The children were not identified and were apparently unaware of the exploitation.

The level of indecency was described by the sentencing judge as ‘in the bottom tier of child exploitation images’.

The defendant had a lengthy criminal history which included convictions for drug and dishonesty offences as well as breaches of court orders. He had not previously been convicted of sexual offences. The defendant had some mental health issues and was employed on a farm.

The defendant was sentenced to 12 months imprisonment, to be served by way of an intensive correction order.

Case study

R v BAG

The defendant pleaded guilty to two counts of making child exploitation material and one count of possessing child exploitation material.

The defendant took two videos on his mobile telephone of the 15-year-old-daughter of his partner. They were taken through the bathroom window on two separate occasions and the child was naked. By the time the videos were discovered by his partner, the defendant had deleted them; however, they were saved in a folder of deleted items in his mobile telephone.

The defendant had no previous convictions, was employed, suffered sexual abuse as a child, suffered from depression and abused alcohol and cannabis.

With respect to the two counts of making child exploitation material, the defendant was sentenced to 12 months imprisonment, wholly suspended, with an operational period of two years. On the count of possessing child exploitation material, the defendant was made subject to a probation order for two years, with special conditions that he undertake counselling and treatment for substance abuse, sexual offending and ‘self-regulation, cognitive distortions, permissive behaviour and relapse prevention’.
Case study

R v SCI; Ex parte Attorney-General (Qld)\(^\text{13}\)

The defendant pleaded guilty to one count of making child exploitation material and one count of distributing child exploitation material.

The defendant had a daughter aged 12 years. On five different occasions, she took a series of photographs of the child. In three photographs, the child wore underwear; in six photographs, the child was naked in the shower; in another six or eight photographs, the child’s vaginal area was depicted—one in which the child held the labia open. The defendant told her daughter the photographs of her vaginal area were needed to show a doctor. Other photographs, the defendant told her, would be used for a photograph album she was making for her. The defendant occasionally tried to entice her to cooperate by promising money or books.

The defendant lived with her husband, her daughter and a son, but was having an affair with another man (B). Some of the photographs of the child were sent to B by the defendant over three occasions. B maintained he was shocked by the photographs and deleted them; however, the defendant told a psychiatrist she had sent them at B’s instigation.

The defendant was aged 37 or 38 years old at the time of the offences, had previous convictions for fraud-related matters including the receipt of family tax benefit and a separate offence of taking money from her employer. The defendant had served a period of actual custody for the latter conviction. She was in custody at the time she was charged with the child exploitation material offences. There was a delay of two years between the date of complaint and the date of the defendant being charged. She had undertaken psychological and drug counselling.

The defendant was placed on a two-year probation order in respect of the making child exploitation material offence. She was sentenced to two years imprisonment, wholly suspended, with an operational period of three years for the offence of distributing child exploitation material. Convictions were recorded on both counts. The Attorney-General appealed on the basis of the inadequacy of the sentence. The appeal was successful regarding the sentence imposed for the offence of distributing child exploitation material, to the extent that the operational period was increased from three years to five years.

Those cases all attracted non-custodial sentences. They can be contrasted with cases such as R v Goodwin; ex parte Attorney-General (Qld)\(^\text{14}\) and R v Tahirij\(^\text{15}\), summarised by means of case studies in sections of this report above, where the making of the material variously involved breaking into homes to make indecent recordings, hacking into the victim’s computer to gain control of a webcam and extorting the girl to perform sexual acts. Goodwin was also convicted of contact offending against four children. Head sentences of eight years imprisonment were imposed in each case, with Goodwin eligible for parole after two years and four months (after a plea of guilty), and Tahiraj after four years (after a trial).

Having now seen examples of conduct even more serious than that in Goodwin and Tahiraj, including in the case studies involving Rivo (who paid for, and directed, appalling live-streamed abuse of children in the Philippines), McCoole (discussed at length above), and Newton and Truong (the so-called ‘two dads’ who abused and allowed the abuse by others of their adopted two-year-old son), the Commission considers that there is a need to reintroduce a distinction in maximum penalties between possessing and distributing child exploitation material, and producing it. The Commission also considers that there is a need for strengthened maximum penalties for those who create new material for the market.

In addition to fulfilling the demand for new and more sickening content, the global nature of the market will sometimes mean that it is not possible for substantive contact offences to be proved against offenders in Queensland. That means that the original intent of Parliament—that offences in 228A (involving a child)
and section 228B (making child exploitation material) be complimentary to substantive offences (such as indecent treatment of a child and rape)—can be defeated. In such cases, charges under those provisions, and appropriate maximum penalties, should be capable of standing alone to provide adequate deterrence and punishment to those in the most serious category of producers of child exploitation material.

It is also noteworthy that the Commission found no case where a charge under section 228A (involving a child in making child exploitation material) had been laid that could not have been dealt with under section 228B (making child exploitation material) of the Code. The distinction made between involving a child in making child exploitation material, and making child exploitation material, seems to have its genesis in the long-outdated scheme established by the Classification of Computer Games and Images Act 1995 and summarised above. There was no explanation for the distinction then, and there was none in 2005 when sections 228A and 228B were introduced.

Taking account of the party provisions in sections 7, 8 and 9 of the Code and the extended jurisdiction provision in sections 12, 13 and 14, there seems to be no conceivable set of circumstances where involving a child in making child exploitation material would not also constitute making child exploitation material. In those circumstances, when undertaking a review of these provisions in accordance with other recommendations, it might be considered that section 228A is superfluous and should be repealed.

**Recommendation**

The Commission recommends that:

4.5 The Queensland Government amend the Criminal Code by increasing the maximum penalty for sections 228A (Involving child in making child exploitation material) and 228B (Making child exploitation material) from 14 years to 20 years imprisonment.

4.6 The Queensland Government amend the Criminal Code to include a circumstance of aggravation for each of the child exploitation material-related offences in sections 228A, 228B, 228C and 228D.

The circumstances of aggravation would apply to any new offence (in relation to administrators of child exploitation websites, those who encourage their use and those who provide advice to avoid detection) enacted in accordance with recommendation 4.4.

The circumstance of aggravation would apply when the Darknet, or other hidden network, or anonymising service was used in the commission of the relevant offence. The terminology used to describe such networks and anonymising services would need to be framed in such a way as to survive the evolution of technology.

The new circumstance of aggravation will increase the maximum penalty for sections 228A and 228B to 25 years imprisonment (see recommendation 4.5 which proposes increasing the simpliciter penalty from 14 years to 20 years imprisonment). The new circumstance of aggravation will increase the maximum penalty for sections 228C and 228D from 14 years to 20 years imprisonment.

**Sexual servitude and deceptive recruitment**

As to a possible inadequacy in the State framework, albeit not strictly within the area of online child sex offending, the Commission became aware that Queensland and Tasmania are the only states not to have enacted sexual servitude and deceptive recruitment offences.
There are a number of international conventions and treaties to which Australia is a party which relate to the rights and protection of, and the suppression of trafficking in, women and children. Some of these date back to the 1920s.16

In 1990, the Law Reform Commission of Australia conducted a review and recommended the introduction of federal laws in line with Australia’s obligations under the treaties and conventions to abolish slavery under the Convention to Suppress the Slave Trade and Slavery, 1926 and the United Nations’ Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery, 1956.

In 1997, the then Model Criminal Code Officers Committee (MCCOC) was asked by the Australian Government to review a proposal to enact laws dealing with slavery. As a result of this review the Committee recommended that provisions be introduced into the Commonwealth Criminal Code dealing with slavery, sexual servitude and deceptive recruiting for sexual services.

In 1999, the Criminal Code Amendment (Slavery and Sexual Servitude) Act 1999 (Cth) was enacted which inserted Division 270 into the Criminal Code (Cth). The new offences included section 270.3 (Slavery), section 270.6 (Sexual servitude) and section 270.7 (Deceptive recruitment for sexual services). The new offences only related to offences focused on sexual exploitation. Prior to this, there were no specific offences relating to trafficking or trafficking practices in Australian law. The law on slavery and the slave trade in Australia had been governed by a number of British Imperial Acts.

Complimentary provisions were enacted by the other states and territories, with South Australia being the first to enact the provisions in June 2000, followed by the ACT in March 2001. New South Wales enacted its provisions in March 2002, the Northern Territory in May 2002 and both Western Australia and Victoria in April and May 2004, respectively. The state and territory legislation applies where an offender operates wholly within Australia and the services provided by their victims are provided wholly within Australia.

The United Nations’ Convention against Transnational Organised Crime was effective from September 2003 and was ratified by Australia in May 2004. As a supplementary protocol, the United Nations’ Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children was ratified by Australia in 2005. In combination, this convention and protocol provide a framework for international cooperation in investigating and prosecuting human trafficking.

Australia’s obligations under the protocol were ultimately achieved by the enactment of the Criminal Code Amendment (Trafficking in Persons) Act 2005 (Cth). That Act inserted Division 271, which creates offences relating to the international and domestic trafficking of persons and children. The Act also made some amendments to offences contained in Division 270 of the Criminal Code.

A research brief prepared in 2011 by the Queensland Parliamentary Library (Number 2011/08), entitled ‘Human Trafficking: Australia’s Response’, referred to the fact that, despite Queensland and Tasmania being without these offence provisions, the Queensland Criminal Code includes the offences of sections 217 (Procuring a young person for carnal knowledge) and 218 (Procuring sexual acts by coercion), as well as a range of other offences which may be applicable, for example, rape, sexual assault and assault offences.

Following that, a further raft of amendments were made when the Crimes Legislation Amendment (Slavery, Slavery-like Conditions and People Trafficking) Act 2013 (Cth) was enacted in February 2013. New offences relating to forced labour, forced marriage, harbouring a person in connection with trafficking, trafficking for the purpose of organ removal and debt bondage were introduced. In addition, the offences of sexual servitude and deceptive recruiting for sexual services were amended to apply to any type of labour or services, not just those with a sexual aspect.

The amended servitude (270.5) and deceptive recruiting (270.7) provisions are subject to the extended geographical jurisdiction set out in section 15.2 – Category B. The extended jurisdiction ensures that the offence provisions capture the conduct of Australian citizens, residents or corporations overseas. The Category B jurisdiction will also capture offending conduct if it occurs wholly within Australia:
15.2 Extended geographical jurisdiction – category B

(1) If a law of the Commonwealth provides that this section applies to a particular offence, a person does not commit the offence unless:

(a) the conduct constituting the alleged offence occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship.

In those circumstances there seems to be no gap in Queensland’s legislative framework in respect of servitude and deceptive recruitment involving children.

Access to stored material by law enforcement

The QPS and CCC brought to the Commission’s attention a vulnerability in the capacity of police to access electronically stored data that is protected by passwords and encryption tools. Access to such data is essential for the detection and investigation of online child sex offending in a world of increasingly sophisticated offenders who use encryption, anonymous proxies and kill switches to avoid detection. 18

The Police Powers and Responsibilities Act 2000 currently allows QPS officers to apply to a magistrate or judge for an order, to be included in a search warrant, for a person to give a police officer access to a ‘storage device’ as well as information necessary to gain access to ‘stored information’.

Section 154 (Order in search warrant about information necessary to access information stored electronically) of the Act provides:

(1) If the issuer is a magistrate or a judge, the issuer may, in a search warrant order the person in possession of access information for a storage device in the person’s possession or to which the person has access at the place –

(b) to give a police officer access to the storage device and the access information necessary for the police officer to be able to use the storage device to gain access to stored information that is accessible only by using the access information; and

(c) to allow a police officer given access to a storage device to do any of the following in relation to stored information stored on or accessible only by using the storage device:

(i) use the access information to gain access to the stored information;

(ii) examine the stored information to find out whether it may be evidence of the commission of an offence;

(iii) make a copy of any stored information that may be evidence of the commission of an offence, including by using another storage device.

In this section - ‘storage device’ means a device of any kind on which information may be stored electronically.

‘access information’ means information of any kind that is necessary for a person to use to be able to access and read information stored electronically on a storage device.

‘stored information’ means information stored on a storage device.

Section 154 of the Act was inserted by the Police Powers and Responsibilities and Other Acts Amendment Act 2006, which was enacted on 1 June 2006. The Explanatory Memorandum states:

It is considered that this amendment is essential to ensure police officers have sufficient powers to investigate persons who engage in activities such as paedophilia, drug trafficking and identity fraud. In many instances, access to information stored on a suspect’s computer, electronic teledex, mobile
phone or similar electronic device is protected by a password or the information is encrypted. In the absence of a password or decryption code, it is often impossible to obtain the stored evidence to prosecute an offender. The requirement to provide the password or decryption code to a computer or mobile phone is not a telecommunications interception, as access will only be gained to data that has already been downloaded or received, e.g. files stored on a DVD, CD or the hard disk of a computer or SMS messages held on the storage space of a mobile phone. Therefore, it is considered that the provision of a power to require a person to provide a password or decryption code that may lead to the gathering of evidence of a serious criminal offence is a matter in the public interest and will stop criminals from escaping prosecution merely because crucial evidence is initially concealed electronically from police.19

Section 154 of the Act does not create an offence and therefore does not prescribe any penalty for the failure or refusal to provide the necessary access information. However, section 156(3) states that the warrant must articulate that the failure, without reasonable excuse, to comply with the order may be dealt with under section 205 of the Criminal Code.

Section 205 of the Criminal Code creates the offence of disobedience to a lawful order issued by a statutory authority. This is the only recourse available to law enforcement when a person fails or refuses to provide investigating police with a means to access his or her computer or device. The maximum penalty is imprisonment for up to one year.

Section 205 – Disobedience to lawful order issued by statutory authority

(1) Any person who without lawful excuse, the proof which lies on the person, disobeys any lawful order issued by any court of justice, or by any person authorised by any public statute in force in Queensland to make the order, is guilty of a misdemeanour, unless some mode of proceeding against the person for such disobedience is expressly provided by statute, and is intended to be exclusive of all other punishment.

(2) The offender is liable to imprisonment for 1 year.

Section 205 covers a very broad range of ‘disobedience’, for example against a civil order for a small amount of compensation to the kind of conduct under consideration here. It acts as a kind of ‘catch-all’ provision for failing to comply with lawful orders.

Statistics relating to the use of section 154 warrants (and equivalent)

Again, the available data was unhelpful in determining how often a suspected child exploitation material offender has refused to comply with an order to provide ‘access information’, and in such cases, what penalty applied.

The Commission was told that the QPS could not accurately determine how many warrants, which included an order under section 154, were either sought or issued.20 Taskforce Argos procedures, however, require that all applications for search warrants include an application for an order under section 154. In the period from 1 January 2012 to July 2015, Taskforce Argos officers were issued 260 search warrants.

The QPS does not hold records that might show the number of instances of non-compliance with an order issued under section 154.

The statistics provided by the QPS indicate that 62 people have been charged with an offence against section 205 of the Criminal Code in the period from 1 January 2012 to 30 June 2015. Of those, 47 matters are the subject of current judicial proceedings, charges against three people were dismissed or discontinued, and 12 people have had their matters finalised. The range of sentences imposed on those 12 people included 75 hours of community service, fines ranging from $50 to $1,500 and short terms of imprisonment (one month, five months and six months, in all cases pre-sentence custody was declared as time already served under the sentence).
The Queensland Sentencing Information Service (QSIS) records statistics showing that four offenders were convicted in the Magistrates Court under section 205(1) and each received a fine ranging from $300 to $1,500. In all cases a conviction was not recorded.21 The facts of these matters are not able to be discerned so that it is unknown if the prosecutions relate to failures to comply with orders under section 154 of the Police Powers and Responsibilities Act. The four convictions occurred over a four-year period from January 2011 to December 2014.

Only one offender has been dealt with in the District Court for an offence under section 205 Criminal Code in the period from January 2008 to December 2014. The offence related to a breach of a child protection order rather than for refusing to provide ‘access information’.

The QSIS statistics also show that two offenders were convicted in the Magistrates Court of an offence under section 3LA (Person with knowledge of a computer system to assist etc) of the Crimes Act 1914 (Cth). Each received a fine of $500 with convictions recorded. The relevant reporting period was from January 2011 to December 2014.

Information taken from the Annual Reports of the Commonwealth Director of Public Prosecutions indicate that over the period 1 July 2011 to 30 June 2014, seven charges under section 3LA of the Crimes Act 1914 (Cth) have been prosecuted across the nation.22 There is no way to determine from this information how many offenders were based in Queensland.

Those statistics further demonstrate the need for an independent statistics and research body. The number of suspects who refuse to provide ‘access information’ under a section 154 order seems to be small, and the penalties imposed for failing to comply are low. However, the consequences for law enforcement are potentially great if such a failure to comply prevents detection or investigation of offending that might involve the abuse of children, or prevent the identification of victims.

The Commission was informed of one particular investigation that has been thwarted by a refusal to provide ‘access information’. That investigation involves allegations of serious, contact offending against unknown victims by a person who had the potential to occupy positions of trust in the community.

The inadequacy of section 154 of the Police Powers and Responsibilities Act and section 205 of the Criminal Code

The problem identified by the QPS is that an online child sex offender will usually be exposed to a far greater penalty for offences involving sexual abuse against children, and/or offending involving child exploitation material, than for refusing to comply with an order that would allow access to information that might convict them. In those circumstances, there is no real incentive for a person to comply with the warrant requirements or, in other words, no effective deterrence.

The more fundamental problem identified by the CCC is that the Crime and Corruption Act 2001 is altogether without an equivalent search power.

In its submission to this Commission, the CCC proposed a similar, but appropriately updated, provision to section 154 of the Police Powers and Responsibilities Act be included in Chapter 3, Parts 2 and 3 of the Crime and Corruption Act 2001.23 The submission proposed the enhancement of section 154 of the Police Powers and Responsibilities Act to reflect new developments in technology and made suggestions in that regard. The submission made reference to the powers contained in section 3LA of the Crimes Act 1914 (Cth) and section 465AA of the Crimes Act 1958 (Victoria).

Section 3LA (Person with knowledge of a computer system to assist etc.) of the Crime Act 1914 (Cth) provides:

(1) A constable may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a constable to do one or more of the following:

(a) Access data held in, or accessible from, a computer storage device that:

(i) is on the warrant premises; or
(ii) has been moved under subsection 3K(2) and is at a place for examination or processing; or

(iii) has been seized under this Division;

(b) Copy data held in, or accessible from, a computer, or a data storage device, described in paragraph (a) to another storage device;

(c) Convert into documentary form or another form intelligible to a constable:

(i) data held in, or accessible from, a computer, or data storage device, described in paragraph (a); or

(ii) data held in, or accessible from, a computer, or data storage device, described in paragraph (b); or

(iii) data held in a data storage device removed from warrant premises under subsection 3L(1A).

(2) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device; and

(b) the specified person is:

(i) reasonably suspected of having committed the offence stated in the relevant warrant; or

(ii) the owner or lessee of the computer or device; or

(iii) an employee of the owner or lessee of the computer or device; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer or devise; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

(c) the specified person has relevant knowledge of:

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in, or accessible from, the computer or device.

(3) If:

(a) the computer or data storage device that is the subject of the order is seized under this Division; and

(b) the order was granted on the basis of an application made before the seizure;

the order does not have effect on or after the seizure.

Note: An application for another order under this section relating to the computer or data storage device may be made after the seizure.

(4) If the computer or data storage device is not on warrant premises, the order must:

(a) specify the period within which the person must provide the information or assistance; and

(b) specify the place at which the person must provide the information or assistance; and

(c) specify any conditions (if any) determined by the magistrate as the condition to which the requirement on the person to provide the information or assistance is subject.
(5) A person commits an offence if the person fails to comply with the order. Penalty for contravention of this subsection: Imprisonment for 2 years.

Section 465AA of the *Crimes Act 1958* (Vic) was enacted in 2014 and largely mirrors the Commonwealth provision, with the following additions:

- the application for an order (requiring assistance) must be made by a police officer above the rank of senior sergeant – subsection 465AA(2)
- the application may be made at the same time the application is made for a warrant, or any time after the issue of the warrant – subsection 465AA(4)
- before issuing the order, the Magistrate must be satisfied that there are reasonable grounds for suspecting that data held in, or accessible from, a computer, or data storage device will afford evidence as to the commission of an indictable offence – subsections 465AA(5)(a) and (5)(b)
- the provision explicitly excludes the application of the privilege against self-incrimination – subsection 465AA(6)
- there is an obligation for police officers to have informed a person of the terms of the order, and that failure to comply constitutes an indictable offence punishable by imprisonment, before an offence can be established – subsections 465AA(9)(b)
- the maximum penalty is five years imprisonment - subsection 465AA(10).

It is later recommended that amendments to section 154 of the *Police Powers and Responsibilities Act (Qld)* be modelled on section 465AA Crimes Act (Vic) and therefore the provision is set out in full below:

**465AA Power to require assistance from person with knowledge of a computer or computer network**

(1) This section applies if a magistrate has issued a warrant under section 465 in relation to a building, receptacle, place or vehicle (warrant premises).

(2) The Magistrates’ Court may, on the application of a police officer of or above the rank of senior sergeant, make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a police officer to do one or more of the things specified in subsection (3).

(3) The things are-

(a) access data held in, or accessible from, a computer or data storage device that-

(i) is on warrant premises; or

(ii) has been seized under the warrant and is at a place other than warrant premises;

(b) copy to another data storage device data held in, or accessible from, a computer, or data storage device, described in paragraph (a);

(c) convert into documentary form or another form intelligible to a police officer-

(i) data held in, or accessible from, a computer, or data storage device, described in paragraph (a); or

(ii) data held in a data storage device to which the data was copied as described in paragraph (b).

(4) An application may be made under subsection (2) at the same time as an application is made for the warrant under section 465 or at any time after the issue of the warrant.

(5) The Magistrates’ Court may make the order if satisfied that-

(a) there are reasonable grounds for suspecting that data held in, or accessible from, a computer, or data storage device, described in subsection (3)(a) will afford evidence as to the commission of an indictable offence; and
(b) the specified person is-
   (i) reasonably suspected of having committed an indictable offence in relation to which the warrant was issued; or
   (ii) the owner or lessee of the computer or device; or
   (iii) an employee of the owner or lessee of the computer or device; or
   (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or
   (v) a person who uses or has used the computer or device; or
   (vi) a person who is or was a system administrator for the computer network of which the computer or device forms or formed a part; and

(c) the specified person has relevant knowledge of-
   (i) the computer or device or a computer network of which the computer or device forms or formed a part; or
   (ii) measures applied to protect data held in, or accessible from, the computer or device.

(6) A person is not excused from complying with an order on the ground that complying with it may result in information being provided that might incriminate the person.

(7) If-
   (a) the computer or data storage device that is the subject of the order is seized under the warrant; and
   (b) the order was granted on the basis of an application made before the seizure- the order does not have effect on or after the completion of the execution of the warrant.

Note: an application for another order under this section relating to the computer or data storage device may be made after the completion of the execution of the warrant.

(8) If the computer or data storage device is not on warrant premises, the order must-
   (a) specify the period within which the person must provide the information or assistance; and
   (b) specify the place at which the person must provide the information or assistance; and
   (c) specify the conditions (if any) to which the requirement to provide the information or assistance is subject.

(9) A person commits an offence if-
   (a) the person has relevant knowledge of-
       (i) the computer or data storage device or a computer network of which the computer or data storage device forms or formed a part; or
       (ii) measures applied to protect data held in, or accessible from, the computer or data storage device; and
   (b) the person is informed by a police officer-
       (i) of the order made under this section and of its terms; and
       (ii) that it is an indictable offence punishable by imprisonment to fail to comply with the order; and
   (c) the person fails to comply with the order without reasonable excuse.
(10) A person who commits an offence against subsection (9) is liable to level 6 imprisonment (5 years maximum).

(11) In this section access, data, data held in a computer and data storage device have the meanings given by section 247A(1).

Both section 3L of the Crimes Act 1914 (Cth) and section 465AA of the Crimes Act 1958 (Vic) allow for orders to be made for a ‘specified person to provide information or assistance that is reasonable and necessary’ to allow police to do one or more specified things. There is no equivalent requirement of reasonableness under section 154 of the Police Powers and Responsibilities Act (Qld).

The Commonwealth and Victorian provisions also include powers additional to those conferred by section 154 of the Police Powers and Responsibilities Act, including the power to require a person to provide police with passwords to ‘unlock’ encrypted data in circumstances where a computer or storage device has been seized under the warrant and is no longer at the warrant premises. That means that if a forensic analysis determines a level of encryption which was not obvious at the time of the search warrant, the opportunity to demand access information in respect of data stored on, or accessible from, the computer or storage device is not lost.

‘Warrant premises’ under section 465AA Crimes Act 1958 (Vic) importantly includes a ‘receptacle’ as well as a building, place or vehicle.

In addition, a ‘specified person’ (which includes but is not limited to the person suspected of committing the offence) who has relevant knowledge of the computer, device, or network, or measures applied to protect data held in, or accessible from the computer or device, an order for assistance may be issued to that person; for example, the administrator of a network.

Another significant inadequacy in respect of section 154 of the Police Powers and Responsibilities Act is that its application is limited to ‘stored information’ which means information stored on a storage device. A ‘storage device’ is a device of any kind on which information may be stored electronically [emphasis added].

To remove any doubt about the accessibility of data held in a ‘cloud’ storage service or similar, both the Commonwealth and Victorian provisions refer to ‘data held in, or accessible from, a computer or data storage device’ [emphasis added]. The definitions of ‘data held in a computer’ in the Commonwealth and Victorian legislation contemplate a wider application to computer information held in a storage device on a network of which the computer forms a part.24 The Victorian legislation defines ‘data’ to include information in any form, and any part of a program.

Western Australia is the only other Australian state to have enacted a similar provision allowing for a person to be ordered to provide access information for a computer and device.25 The Criminal Investigations Act 2006 (WA) provides that a Magistrate may make a ‘data access order’ requiring a person who is suspected of committing a serious offence, to provide information or assistance to allow police to gain access to a ‘data storage device’. Disobedience of the order attracts a maximum penalty of five years imprisonment, or on summary conviction, imprisonment for a maximum of two years.

It is clear that section 154 of the Police Powers and Responsibilities Act provides a powerful tool for investigators, but one which also impinges on a citizen’s privilege against self-incrimination. It is also clear however, that sex offenders, including contact offenders and those who participate in the child exploitation material market, might avoid more serious consequences by refusing to provide police officers with access to incriminating data held in, and accessible from, computers and other storage devices.

Currently, the power provided by section 154 of the Police powers and Responsibilities Act, combined with the offence provision in section 205 of the Criminal Code, provide insufficient disincentive to offenders who have more to lose by complying.

The Commission further considers that section 154 of the Act requires updating to address new technologies and allow for orders for assistance to be made after computer and storage devices have been seized for examination or analysis. Section 465AA of the Crimes Act (Vic) provides a good template for change;
incorporating key aspects of the Commonwealth provision while requiring the issuing Magistrate to be satisfied, on reasonable grounds, that the data sought by police will afford evidence of an indictable offence.

It is not considered appropriate however, that the Police Powers and Responsibilities Act contain the offence provision, which the Commission recommends should be a new, indictable offence carrying a maximum penalty of five years imprisonment, and seven years imprisonment when a circumstance of aggravation applies.

The circumstance of aggravation would apply when an offender has been found to be in possession of child exploitation material (for example on an unencrypted storage device) but refuses to provide access to other computers, parts of a computer, or storage devices.

Since it would be an indictable offence, the offence should properly be inserted into the Criminal Code, perhaps immediately following the existing section 205 to create a new section 205A – Disobedience of a lawful order to provide access information or assistance.

As to the Crime and Corruption Act 2001, the Commission agrees with the CCC submission that Chapter 3, Part 2 should be amended to allow ‘an authorised commission officer’ to seek an order, as part of a search warrant application, for assistance from a person with knowledge of a computer, storage device or network.

In order to engage the offence provision recommended by the Commission, the Crime and Corruption Act would also need to articulate that a failure to comply with such an order may be dealt with under the new provision (suggested section 205A) in the Criminal Code.

Section 91(2) of the Crime and Corruption Act currently provides that if the issuer of a search warrant makes an order under section 88 (an order in a search warrant to provide documents), the search warrant must state that failure, without reasonable excuse, to comply with the order may be dealt with under section 205 Criminal Code. A similar provision might require that the warrant state that a failure to comply with an order to provide assistance and information, may be dealt with under section 205A of the Criminal Code.

The CCC further submitted that Chapter 3, Part 3, dealing with immediate search powers and post-search approval orders should similarly be amended. Currently, section 96 of the Act allows an authorised commission officer to search a place without a warrant to prevent the loss of evidence. This is permitted if the officer reasonably suspects that evidence may be concealed or destroyed unless the place is immediately entered and searched. After a place has been entered, section 97 requires the officer to make an application to a magistrate for a post-search approval order. Under section 98, the magistrate may make the post-search approval order only if satisfied there were reasonable grounds for the officer to believe that evidence may have been concealed or destroyed if the place was not immediately entered and searched. The magistrate must also be satisfied, having regard to the nature of the evidence found during the search, that it is in the public interest to make the order.

Given that the power to require assistance will usually represent a significant encroachment on the rights of the citizen, particularly the privilege against self-incrimination, this Commission does not consider it appropriate that the power be available unless a magistrate has been satisfied in advance that there are reasonable grounds for conferring it. Further, those investigating online child exploitation material will, in majority of cases, have prior knowledge sufficient to understand the need for a search warrant, and a basis for same to be issued under Chapter 3, Part 2 of the Crime and Corruption Act.

In other cases, the CCC has the power to order a person to answer questions in a coercive hearing. Section 199 of Crime and Corruption Act provides strict punishment provisions for contempt, including mandatory minimum terms that must be served wholly in a corrective services facility.
**Recommendation**

The Commission recommends that:

**Amendments to the Police Powers and Responsibilities Act 2000**

4.7 The Queensland Government amend section 154 (Order in search warrant about information necessary to access information stored electronically) of the Police Powers and Responsibilities Act 2000 so that:

- ‘stored information’ includes information accessible by a computer or storage device (for example from a ‘cloud’ storage service); and
- an application for another order may be made after the seizure of a computer or storage device; and
- an order may contain conditions for the provision of access information at some future time when the computer or storage device is not on the premises.

In developing the amendments regard should be had to section 465AA of the Crimes Act 1958 (Vic).

**Amendments to the Crime and Corruption Act 2001**

4.8 The Queensland Government amend Chapter 3, Part 2 (Search warrants generally) of the Crime and Corruption Act 2001 to include a provision allowing for the issuer of a search warrant to make orders about information necessary to access information, in the same, or similar, terms as section 154 of the Police Powers and Responsibilities Act, as amended in accordance with recommendation 4.7.

A consequential amendment might also be made to provide that a failure to comply with such an order may be dealt with under the new offence provision in the Criminal Code recommended in 4.9, below.

**Amendments to the Criminal Code**

4.9 The Queensland Government amend the Criminal Code to insert a new offence of failing to comply with an order in a search warrant about information necessary to access information stored electronically (whether made under the Police Powers and Responsibilities Act 2000 or the Crime and Corruption Act 2001). The offence would be an indictable offence, and carry a maximum penalty of five years imprisonment.

The new offence would include a circumstance of aggravation, increasing the maximum penalty to seven years imprisonment, when the specified person is in possession of child exploitation material at the time the search warrant is executed.

Section 552A of the Criminal Code should be amended to provide that the new offence may be heard summarily on the prosecution election.

**Data retention**

The Commission was alerted to an existing gap in laws relating to the type of information required to be retained by Internet and telecommunications service providers, and the length of time for which it is required to be retained.

Detective Inspector Rouse told the Commission that the information that an investigator requires is the same information that is ordinarily kept by ISPs in order to bill their clients, for example, the time and date of access,
the IP address and the subscriber details. Detective Rouse expressed concern that there was no statutory requirement on ISPs to retain this information, known as metadata. Metadata is information about a communication (by telephone or over the Internet), such as the subscriber details, phone numbers of individuals who have called each other, the duration of a phone call, the email address from which a message was sent and the duration of Internet usage. Metadata does not extend to the content or substance of a communication.

Access to metadata by law enforcement agencies is vital to the investigation and identification of individuals engaged within online child exploitation material distribution networks. Other shortcomings in relation to the retention of metadata (specifically, subscriber information) by ISPs were identified as follows:

- there is a lack of consistency amongst ISPs regarding the period of time during which data must be retained
- there is no mandatory minimum level of detail in the type of data that must be retained by ISPs
- ISPs claim to have the inability to provide subscriber information for individuals who access child exploitation using mobile data.

Mr Paul Griffiths echoed Detective Inspector Rouse’s concerns and told the Commission that, often, requests are made to ISPs for data only to be told that the information is not available since request has been made outside the data retention period, or because the information requested is for mobile data.

Mobile data is data accessed by a person using a smartphone, tablet or other portable device from the Internet via a cellular system. Fixed data, on the other hand, is that which is transmitted by a person with a stationary computer or terminal to and from a network.

Until recently, it is apparent that the concerns expressed by law enforcement officers were well-founded. However, on 13 April 2015, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) received Royal Assent and will take effect from 14 October 2015. The Bill received considerable publicity and attracted controversy. It amends the Telecommunications (Interception and Access) Act 1979 to impose a requirement on telecommunications companies, including ISPs, to retain comprehensive telecommunications data (metadata) for two years. The metadata that an ISP will be required to retain is based on the following six categories:

- the identity of the subscriber to a telecommunications service
- identifiers of the source of a communication
- identifiers of the destination of the communication
- the date, time and duration of a communication
- the type of communication (e.g., voice, SMS, MMS or social media usage)
- the location of the equipment used in a communication (e.g., cell tower or wi-fi hotspot location).

The Explanatory Memorandum to the Bill acknowledges the importance of such information to law enforcement agencies. Some activities, including child pornography, are predominantly executed through communications devices such as phones and computers. The TIA Act provides a framework for national security and law enforcement agencies to access the information held by communications providers that agencies need to investigate criminal offences and other activities that threaten safety and security.

Schedule 1 of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 inserts a new Part 5-1A into the Telecommunications (Interception and Access) Act 1979. The types of information that an ISP will be required to retain will be included under the new section 187AA of the Telecommunications (Interception and Access) Act 1979 (Cth). The following table provides a summary:
<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Further description of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service</td>
<td>The following:</td>
</tr>
<tr>
<td></td>
<td>(a) any information that is one or both of the following:</td>
</tr>
<tr>
<td></td>
<td>(i) any name or address information;</td>
</tr>
<tr>
<td></td>
<td>(ii) any other information for identification purposes;</td>
</tr>
<tr>
<td></td>
<td>relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service;</td>
</tr>
<tr>
<td></td>
<td>(b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device;</td>
</tr>
<tr>
<td></td>
<td>(c) any information that is one or both of the following:</td>
</tr>
<tr>
<td></td>
<td>(i) billing or payment information;</td>
</tr>
<tr>
<td></td>
<td>(ii) contact information;</td>
</tr>
<tr>
<td></td>
<td>relating to the relevant service, being information used by the service provider in relation to the relevant service;</td>
</tr>
<tr>
<td></td>
<td>(d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device;</td>
</tr>
<tr>
<td></td>
<td>(e) the status of the relevant service, or any related account, service or device;</td>
</tr>
<tr>
<td>The source of a communication</td>
<td>Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.</td>
</tr>
<tr>
<td>The destination of a communication</td>
<td>Identifiers of the account, telecommunications device or relevant service to which the communication:</td>
</tr>
<tr>
<td></td>
<td>(a) has been sent; or</td>
</tr>
<tr>
<td></td>
<td>(b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.</td>
</tr>
<tr>
<td>The date, time and duration of a communication, or of its connection to a relevant service</td>
<td>The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication):</td>
</tr>
<tr>
<td></td>
<td>(a) the start of the communication;</td>
</tr>
<tr>
<td></td>
<td>(b) the end of the communication;</td>
</tr>
<tr>
<td></td>
<td>(c) the connection to the relevant service;</td>
</tr>
<tr>
<td></td>
<td>(d) the disconnection from the relevant service.</td>
</tr>
<tr>
<td>Type of Information</td>
<td>Further description of information</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| The type of a communication or of a relevant service used in connection with a communication | The following:  
(a) the type of communication;  
Examples: Voice, SMS, email, chat, forum, social media.  
(b) the type of the relevant service;  
Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE.  
(c) the features of the relevant service that were, or would have been, used by or enabled for the communication.  
Examples: Call waiting, call forwarding, data volume usage. |
| The location of equipment, or a line, used in connection with a communication | The following in relation to the equipment or line used to send or receive the communication:  
(a) the location of the equipment or line at the start of the communication;  
(b) the location of the equipment or line at the end of the communication.  
Examples: Cell towers, Wi-Fi hotspots. |

Law enforcement agencies will be able to access this data under the authority of a warrant under the existing provisions of Part 3-3 of the *Telecommunications (Interception and Access) Act 1979* (Cth).

The Commission is satisfied that the amendments allay the concerns expressed.

**International ISPs**

Mr Griffiths referred to an additional problem encountered with some overseas-based social networking companies and ISPs. Where an organisation is based outside of Australia (even when it has an Australian office), the provider might refuse to provide Queensland law enforcement officers with requested information. In that case a request must be made under the *Mutual Assistance in Criminal Matters Act 1987* (Cth) and that can take considerable time. In the meantime, critical data (that might help locate a child victim, for example) might be lost because of short retention periods mandated in other jurisdictions.

The following diagram shows the complex process which, the Commission was told, can take in the order of 18 months.
Crime allegedly committed against an Australia law

Law enforcement agency identifies evidence which is located overseas

If there is no appropriate alternatives, agency considers what form of mutual assistance (MA) is required.

Australia can request the following types of assistance

- Take evidence and production of documents
- Search and seizure
- Travel arrangements for persons including prisoners to Australia
- Proceeds of crime proceedings
- Other types of assistance not specified in the Mutual Assistance Act

Law enforcement or prosecution agency completes a MA request questionnaire and sends it to Attorney-General’s Department (AGD). AGD uses the information in the questionnaire to draft the request.

AG (or AG’s delegate) approves the request

AGD transmits the request to the foreign country and liaises with the Central Authority in the foreign country about the progress of the request and any further information required.

Foreign country considers Australia’s request and provides the assistance sought.

AGD considers the requirements of the Foreign Evidence Act. AGD will seal the material at the agency’s request if it is an admissible form. AGD transfers any material obtained to the requesting agency.

Requesting agency uses the material in investigation and prosecution of the alleged crime or in related proceeds of crime proceedings.

Design amended for style.

Mr Griffiths suggested consideration of a mechanism by which a court order issued in Australia for information to be provided by an ISP becomes enforceable in the country in which the information is held.36

Any such mechanism would be for the federal government to consider, and would be unlikely to be enforceable. The issue underscores the importance of maintaining the kind of transnational relationships Taskforce Argos has already established (see the following section on responses to organised crime) and forging new ones where necessary.

Blocking child exploitation material

Given the information received from the QPS and the CCC showing the enormous trade in child exploitation material, the Commission resolved to look into the possibilities for blocking offending websites and content.
One way to stem the distribution of child exploitation material on the Internet is by ISPs blocking access to such websites. Section 313(3) of the Telecommunications Act 1997 requires carriers and carriage service providers in Australia to give officers and authorities of the Commonwealth, and of the states and territories, such help as is reasonably necessary to:

- enforce the criminal law and laws imposing pecuniary penalties;
- assist the enforcement of the criminal laws in force in a foreign country;
- protect the public revenue; and/or
- safeguard national security.

The provision does not specifically prescribe the process for blocking a website by an ISP. However, the provision, which commenced in 1997, has been used by state and federal agencies to gain the assistance of ISPs in blocking access to websites where such help has been shown to be reasonably necessary and is consistent with the broader obligation of the industry to comply with the law.37

Under section 313(5) of the Telecommunications Act 1997, an ISP is not liable for an act done or omitted in good faith in compliance with a request under section 313.

**Committee Inquiry**

In March 2013, the Australian Securities and Investment Commission (ASIC) used the powers available under section 313(3) of the Telecommunications Act 1997 to prevent access to websites involved in financial crime. As an inadvertent consequence, a number of legitimate online services were disrupted. That raised issues within the community regarding the legitimacy of this law enforcement tool. Accordingly, the then Minister for Communications, the Hon Malcolm Turnbull, MP, referred the use of section 313(3) of the Telecommunications Act 1997 to the Standing Committee on Infrastructure and Communications for review and report (the Committee Inquiry).

The Committee was tasked with considering:

- Which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians;
- What level of authority should such agencies have in order to make such a request;
- The characteristics of illegal or potentially illegal online services which should be subject to such requests; and
- What are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:
  - Legislation;
  - Regulations; or
  - Policy.

The Committee Inquiry received 21 submissions from law enforcement agencies, community groups, industry bodies and private citizens regarding the use of the provision and undertook six public hearings. After considering the material, the Committee made the following recommendation:

The adoption of whole-of-government guidelines for government agencies, including:

- the development of agency-specific internal policies consistent with the guidelines;
- clearly defined authorisations at a senior level;
- defining activities subject to disruption;
- industry and stakeholder consultation;
- the use of stop pages, which identify the agency requesting the block, the reason for the block, an agency contact and an avenue for review.
- public announcements where appropriate;
- review and appeal processes; and
- reporting arrangements.

On 1 June 2015, the Committee tabled its report in the House of Representatives. The Government response had not been published at the time of writing this report.

**Usage**

In its submission to the Committee Inquiry, the Department of Communications submitted that the use of this provision by government agencies does not appear to be widespread, with 32 requests made between 2011 and 2013.\(^{38}\) However, the Department of Communications did note that agencies are currently under no obligation to report the use of section 313 as a law enforcement tool.

The majority of requests originated from the AFP as part of its Access Limitation Scheme, which seeks to limit access to a list of websites (the Worst-of list) deemed by Interpol to contain the most severe child exploitation material according to defined criteria. The defined criteria for inclusion on the Worst-of list are:\(^{39}\)

- the children are real (computer generated, morphed, drawn or pseudo images are precluded)
- the ages of the children depicted in sexually exploitative situation are (or appear to be) younger than 13 years
- the abuses are considered severe by depicting sexual contact or focus on the genital or anal region of the child
- the domains have been online within the last three months the domains have been reviewed and found to fulfill the above criteria by at least two independent countries/agencies.

The Access Limitation Scheme originated as a result of the decision by the previous Federal Government to abandon a mandatory Internet filter policy in 2012. The Worst-of list is provided by Interpol to the AFP for dissemination, without alteration, to domestic ISPs. Although a decision by an ISP to participate in the Access Limitation Scheme is voluntary, it is underpinned by a request under section 313(3) of the Telecommunications Act 1997 to block access to websites prescribed in the Worst-of list.

**Limitations**

A criticism surrounding the application by law enforcement agencies of section 313(3) is that the processes lack transparency and accountability. Specifically, if access to a particular website is denied under this provision, it is not apparent which government agency had requested the disruption and which agency to contact to reinstate access in those instances where the blockage had been inadvertent.

As noted by the Department of Communications in its submission to the Committee Inquiry,\(^{40}\) agencies are currently under no obligation to report the use of section 313 to block access to websites, which limits information available to the community in respect of the extent of censorship. It is noted however, that the implementation of the recommendations of the Committee of Inquiry may cause some of these concerns to be addressed.

Another limitation relevant to law enforcement relates to the use of Virtual Private Networks (VPNs), Tor (and other Darknet browsers) and P2P software which are not affected by the use of section 313(3) of the Telecommunications Act 1997, but which provide access for individuals to a growing source of child exploitation material.

Further, Paul Griffiths told the Commission that in his view the effectiveness of blocking websites is limited to preventing casual observers coming across a site that they did not realise would contain child exploitation material. Google has implemented a process whereby a user, who has used a search term recognised as a typical term used for searching child exploitation material, is automatically referred to a page setting out the law with respect to child exploitation material. The page might also refer a user to websites that might provide assistance for psychological problems. Mr Griffiths stated these types of initiatives, while admirable, will not deter a person who is deliberately searching and determined to find child exploitation material online.\(^{41}\)
Blocking material shared on peer-to-peer (P2P) platforms

Detective Inspector Rouse likened the task of investigating and apprehending child exploitation material offenders using P2P platforms to sipping from a fire hose. Such is the extent of that type of offending in Queensland, particularly in the South-East corner of the state. Given that, the Commission was interested to know if material shared on those platforms could be blocked in the same way websites on Interpol’s Worst-of list are currently blocked by ISPs.

Detective Rouse and Paul Griffiths from Argos, and Detective Cameron Burke of the CCC Cerberus Unit agreed that it was possible. All held reservations, though, about the possible effects of creating a need for new material to fill the gap, and driving offenders ‘underground’.

The process that would be engaged to block child exploitation material being shared on P2P platforms is the same as that used to control the circulation of pirated music and films. If ISPs were provided with a database of ‘hash sets’ or ‘PhotoDNA’ data that identifies known child exploitation material files, it is theoretically possible for those files to be blocked. It is also possible, according to Mr Griffiths, for ISPs to engage in ‘port blocking’. That is a process whereby ports, which are identified as being used to transport child exploitation material, are blocked. ‘Port throttling’ is another method of deterring users by making access to files so slow that they are turned away. Flooding a platform with masses of files which purport to be child exploitation material but are not, can also be effective in frustrating (but not stopping) the efforts of would-be child exploitation material offenders.

The clear message from law enforcement officers was that while theoretically possible, blocking content shared on P2P and other ‘surface’ platforms would act only as a temporary deterrent to those intent on finding and sharing child exploitation material, and might have the effect of making law enforcement more difficult by sending frustrated users into the Darknet.

The measures that might be taken to block child exploitation material files available on P2P platforms or other Surface Web websites, bulletin boards or chat rooms, fall for consideration by the federal government. Such measures might simply require an extension of the application of provisions recently introduced by the Copyright Amendment (Online Infringement) Bill 2015 (Cth).

That Bill was passed with bi-partisan support, although not without controversy and opposition, in June 2015. The aim of the amendments is to curb online piracy of films and television programs by allowing copyright holders to apply to a Federal Court judge for an order compelling Australian Carriage Service Providers (CSPs) to block overseas websites, or ‘online locations’ that facilitate (as a ‘primary purpose’) copyright infringement.

Blocking by Australian CSPs will prevent Australian users gaining access to infringing copyright material accessed from those locations and to programs or other tools available at the online locations that facilitate the infringement of copyright. The injunction power only applies to online locations operated outside Australia. Section 115 of the Copyright Act 1968 (Cth) already provides an avenue for action against an online location within Australia.

These anti-piracy measures focus on ‘site blocking’ which is already achieved, at least to some extent, by the cooperation of Australian ISPs blocking Interpol’s Worst-of list. Further, section 313 of the Telecommunications Act 1997, despite its limitations, allows for website blocking. Blocking content on P2P platforms however, requires ISPs (or CSPs) to block individual files (running into the millions) by using hash sets and PhotoDNA (see below), or by port-blocking as Mr Griffiths suggests.

PhotoDNA is a technology developed by Microsoft that computes hash values of images in order to identify alike images. Google, Gmail, Twitter, Facebook and the National Centre for Missing and Exploited Children (NCMEC) use the technology to block child abuse images. Microsoft has recently launched a cloud version of PhotoDNA which is available to download for free from the Azure Marketplace.

The Australian Communications and Media Authority (ACMA) is a federal government statutory body within the Communications portfolio. The ACMA is a regulator, which oversees telecommunications, broadcasting, radio communications and the internet in Australia. An independent statutory office within the ACMA, the
Office of the Children’s eSafety Commissioner was established on 1 July 2015. This office, as part of its many roles, administers a complaints mechanism for Australian residents and law enforcement agencies to report prohibited online content, including child exploitation material. The hotline is known as the eSafety Hotline and is part of a global network of international hotlines, the International Association of Internet Hotlines (INHOPE) that exchanges information on child exploitation material. Other members of the network include the United Kingdom’s Internet Watch Foundation, the United States National Centre for Missing and Exploited Children (NCMEC) as well as organisations from Canada, Russia and Japan.

If child exploitation material is identified as being hosted in Australia, the eSafety Hotline directs the relevant host to remove the content and refers it to a relevant state or territory police force prior to taking this action. If the material is hosted outside of Australia in a country with an INHOPE member, then the eSafety Hotline reports the content to them for rapid law enforcement and for the material to be removed. If the material appears to be hosted in a country that does not have a hotline, then the content is referred to the Australian Federal Police for action to be taken through Interpol.

The Office of the Children’s eSafety Commissioner does not take action to block websites. Nor does it investigate whole websites or domains or actively monitor the Internet.46

Despite the degree of difficulty and the reservations expressed about the ultimate effectiveness of content blocking, the Commission is of the view that all possible measures should be taken to prevent online access to, and distribution of, child exploitation material.

Courts in Queensland recognise that child exploitation material offences are not victimless crimes. The following comments by Clare DCJ in a case involving a particularly large and depraved collection are apt:

General deterrence and denunciation are very important in a case of this kind. The offences are the kind committed at home, alone, behind closed doors, but still they expose children to serious harm. Even though you didn’t touch any child, and even though you weren’t engaged in the commission of any of the crimes depicted in your material, the 50,000 images that you collected recorded the abuse of real children. You had images of the rape and degradation of very small children.

What you did was not just some invasion of their privacy; when you downloaded this material your conduct was an encouragement for the creation of more of the same - the abuse of more children around the world.47

Federal legislation compelling Carriage Service Providers to block access to child exploitation material either by site-, port- or content-blocking, would surely incite less controversy than that successfully passed to deal with breaches of copyright and the rights of artists to fair remuneration. The societal benefits in favour of implementing similar measures to stem the child exploitation material market are obvious and critical, including saving children from harm and directing scant police resources to areas of priority.

**Recommendation**

4.10 The Commission recommends that the Queensland Attorney-General seek to include legislative and other measures apt to block or remove child exploitation material on to the 2015–2016 agenda for the Law, Crime and Community Safety Council.

**Classification of child exploitation material**

In submissions to the Commission, the CCC and the ODPP raised issues relating to the classification of child exploitation material. In interviews conducted by the Commission, officers of the QPS also expressed concerns.
The issues relate to the enormous amount of time it takes police officers, and civilians in the employ of law enforcement agencies, to assign one of six classifications to each of the millions of images found in the possession of offenders. Paul Griffiths, Victim Identification Coordinator, Taskforce Argos, told the Commission that his library of images (used in the victim identification process) contains approximately eight million files. For law enforcement agencies, that task takes resources away from victim identification and the priority of rescuing those children from further harm. For the ODPP, the time taken by police to classify the images and video files often means delays in prosecuting offenders.

The CCC referred to ‘challenges for policing criminal paedophilia due to categorisation of child exploitation material files’, saying:

The 2002 UK case of Regina v Oliver in the Court of Appeal established a scale by which indecent images of children could be categorised. The five point scale was developed by the UK’s sentencing advisory panel and adopted in 2002. The scale is formally known as the SAP scale but in an Australian law enforcement context is referred to as the ‘Oliver Scale’. The Oliver scale has come to be used as a means of categorising images to allow courts to sentence offenders without themselves having to review a sample of the evidence to assess its seriousness.

Reliance on the scale and classification of images within the scale has led to a shift in focus on the seriousness of images, rather than an assessment of an offender’s risk to the community. It also leads to a focus for investigators in assessment and categorisation of images to the detriment of other areas of policing, such as identification of victims.

The classification of images according to an adapted version of the so-called Oliver scale is routinely used by Queensland courts in sentencing child exploitation material offenders. The scale includes the five categories initially developed in R v Oliver, Hartrey and Baldwin [2002] EWCA Crim 2766 (Oliver), as well as a sixth category for indecent depictions of children in animated, cartoon or virtual images:

<table>
<thead>
<tr>
<th>The adapted ‘Oliver’ scale</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Images depicting erotic posing with no sexual activity</td>
</tr>
<tr>
<td>2</td>
<td>Sexual activity between children, or solo masturbation by a child</td>
</tr>
<tr>
<td>3</td>
<td>Non-penetrative sexual activity between adults and children</td>
</tr>
<tr>
<td>4</td>
<td>Penetrative sexual activity between children and adults</td>
</tr>
<tr>
<td>5</td>
<td>Sadism or bestiality</td>
</tr>
<tr>
<td>6</td>
<td>Anime, cartoon or virtual images</td>
</tr>
</tbody>
</table>

The sixth category has its genesis in the case of R v Campbell [2009] QCA 128. The Court of Appeal noted the position taken by the sentencing judge, and not raised on appeal, that the fictional story in question fell within the definition of child exploitation material, and that the ‘someone’ described or depicted in the material need not be a real person but may be a fictional character.

The Criminal Law (Child Exploitation and Dangerous Drugs) Amendment Act 2013 amended the definition of child exploitation material in section 207A of the Criminal Code to include animated and virtual images of a child.

In exercising the sentencing discretion, a court is to have regard to the sentencing principles set out in the Penalties and Sentences Act 1991. Subsection 9(7) of the Penalties and Sentences Act prescribes specific matters to be considered in sentencing an offender for child exploitation material-related offences:
In sentencing a child-images offender, the court must have regard primarily to –

(a) the nature of any image of a child that the offence involved, including the apparent age of the child and the activity shown; and

(b) the need to deter similar behaviour by other offenders to protect children; and

(c) the prospects of rehabilitation including the availability of any medical or psychiatric treatment to cause the offender to behave in a way acceptable to the community; and

(d) the offender’s antecedents, age and character; and

(e) any remorse or lack of remorse of the offender; and

(f) any medical, psychiatric, prison or other relevant report relating to the offender; and

(g) anything else about the safety of children under 16 the sentencing court considers relevant.

In considering subsection 7(a), the court will have reference to the number and nature of images/films in each of the six categories. A table or report will have generally been prepared for the court providing that information as well as a brief description of some of the images/films in each category. That usually obviates the need for a judge to look at any of the material. The same usually applies to prosecution and defence lawyers and clerks.

The Oliver scale was first adopted by Queensland courts in about 2007, and by 2011 the scale was being routinely used in the sentencing process.

Oliver was decided after the UK’s Sentencing Advisory Panel posed a question in relation to offences involving indecent photographs and pseudo-photographs of children, particularly in relation to when the custody threshold should be regarded as having been passed. The Sentencing Advisory Panel also provided advice to the Court which was largely adopted in the decision.

Importantly, the Court in Oliver agreed with the Sentencing Advisory Panel that the two primary factors, which determine the seriousness of a particular offence, are the nature of the indecent material and the extent of the offender’s involvement with it. That proposition is supported by sentencing courts in Queensland, where the quantity and/or level of depravity of material in the worst categories (Categories 4 and 5), and factors including whether an offender has stored and/or distributed material often weigh heavily in deciding the appropriate penalty.

For example, in R v Smith the sentencing judge noted that a significant number of the 1,175 unique images were at the higher end of the scale, meaning that they involved actual harm and injury to the children who were the subject of the images. In R v Sykes, it was noted that although the number of images was ‘relatively modest’ (89), some images were of extremely young children involving exploitation and degradation.

Deterrence remains the paramount sentencing consideration.

In addition to the Oliver scale, various classification scales have been referred to by courts in Queensland and in other Australian jurisdictions. The COPINE scale was developed by researchers at the University of Cork and formed part of the Sentencing Advisory Panel’s advice to the Court of Appeal in Oliver. It has 10 categories, but was adapted by the Court in Oliver and became known as the Oliver scale. The ten categories of the COPINE scale are as follows:
The COPINE Scale

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicative</td>
<td>Non-erotic and non-sexualised pictures showing children in their underwear, swimming costumes from either commercial sources or family albums. Pictures of children playing in normal settings, in which the context or organisation of pictures by the collector indicates inappropriateness.</td>
</tr>
<tr>
<td>2</td>
<td>Nudist</td>
<td>Pictures of naked or semi-naked children in appropriate nudist settings, and from legitimate sources.</td>
</tr>
<tr>
<td>3</td>
<td>Erotica</td>
<td>Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.</td>
</tr>
<tr>
<td>4</td>
<td>Posing</td>
<td>Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organisation suggests sexual interest).</td>
</tr>
<tr>
<td>5</td>
<td>Erotic Posing</td>
<td>Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses.</td>
</tr>
<tr>
<td>6</td>
<td>Explicit Erotic Posing</td>
<td>Pictures emphasising genital areas, where the child is either naked, partially clothed or fully clothed.</td>
</tr>
<tr>
<td>7</td>
<td>Explicit Sexual Activity</td>
<td>Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.</td>
</tr>
<tr>
<td>8</td>
<td>Assault</td>
<td>Pictures of children being subject to a sexual assault, involving digital touching, involving an adult.</td>
</tr>
<tr>
<td>9</td>
<td>Gross Assault</td>
<td>Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation or oral sex, involving an adult.</td>
</tr>
<tr>
<td>10</td>
<td>Sadistic/Bestiality</td>
<td>a. Pictures showing a child being tied, bound, beaten, whipped or otherwise subject to something that implies pain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Pictures where an animal is involved in some form of sexual behaviour with a child.</td>
</tr>
</tbody>
</table>

The Commission found reference to the COPINE scale in some decisions of the New South Wales Court of Criminal Appeal, which has also decided child exploitation material cases using the Oliver scale.

A recent decision by Her Honour Judge Ryrie in the Brisbane District Court refers to another scale, ANVIL (‘which I used to know as the Oliver scale’). Earlier, in 2011, Judge Ryrie had been referred to the ‘Australian Child Exploitation Categorisation Scheme’ which the Commission understands to be a reference to the Child Exploitation Tracking System.

The Australian National Victim Image Library (ANVIL) and the Child Exploitation Tracking System (CETS) adopt essentially the same classification system, using a scale of five categories. The two scales have been referred to (sometimes interchangeably and with reference to the Oliver scale) in a number of recent cases. In 2008, in a joint media release between the AFP and Microsoft, CETS was described as a tool enabling the AFP to work with law enforcement agencies throughout Australian and around the world, to share and
track information relating to online child exploitation and abuse. CETS, however, is no longer supported by Microsoft. The CrimTrac Annual Report 2013–2014, states that while the AFP and CrimTrac are working to identify a replacement solution for CETS, a number of milestones had been achieved. One of those was the implementation of a national standard for the categorisation of child exploitation material.

In conjunction with the AFP and CrimTrac, the QPS began developing ANVIL (which used CETS) in 2010. The database aims to assist police to identify child victims and automate and optimise the process of reviewing images of children who are being sexually abused. Detective Superintendent Cameron Harsley, formerly of the QPS Child Safety and Sexual Crime Unit, said that automation is the key to reducing practitioner exposure to child exploitation material and to increasing victim identification opportunities by focusing investigative resources on newer images where evidence of contact offending is likely to be more prevalent. ANVIL adopts the same five categories used in CETS for classification of files. The categories mirror the Oliver scale.

In conjunction with the AFP and CrimTrac, the QPS began developing ANVIL (which used CETS) in 2010. The database aims to assist police to identify child victims and automate and optimise the process of reviewing images of children who are being sexually abused. Detective Superintendent Cameron Harsley, formerly of the QPS Child Safety and Sexual Crime Unit, said that automation is the key to reducing practitioner exposure to child exploitation material and to increasing victim identification opportunities by focusing investigative resources on newer images where evidence of contact offending is likely to be more prevalent. ANVIL adopts the same five categories used in CETS for classification of files. The categories mirror the Oliver scale.

The QPS hopes that a product called NetClean will supersede CETS and provide a sophisticated tool for identifying and cataloguing child exploitation material. Officers in Taskforce Argos have already taken steps to make the case for the national use of Netclean, and sufficient funding to allow that to happen. Those efforts have the support of the Commission.

Data fed into NetClean will populate an international database, called Project Vic. Project Vic provides a database of millions of known images and hash sets. The database allows law enforcement users to know which images are likely not to have been seen previously and therefore are worthy of closer inspection. Project Vic compliments Interpol’s International Child Sexual Exploitation Image Database (ICSE DB). The ICSE DB is a global victim identification database which uses sophisticated image comparison software to make connections between victims, abusers and places. It helps investigators determine if an image has already been identified and/or investigated. The database contains ‘baseline’ material, which is material that is illegal according to a two-category standard (legal or illegal).

The practical effect of the Netclean ‘solution’ is that it obviates the need for law enforcement officers to look at every image in an offender’s collection for the purpose of trying to identify victims. For example, in a collection of 10,000 images, Netclean might identify that 8,000 images have previously been seen and catalogued. That allows officers to focus on the remaining 2,000 images.

The use of the adapted Oliver scale in the sentencing process creates a number of unnecessary complications. Firstly, in the example used above, it means that someone still needs to look at the 8,000 images already catalogued according to the two-category standard and apply the appropriate ‘Oliver’ classification. That is considered by Taskforce Argos to be a misdirection of resources that could be used in investigations, including to identify victims of child sexual abuse.

Secondly, Paul Griffiths said that the QPS use of that database, as well as the capacity to contribute, are complicated by the fact that there is no correlation between the current classification scale (six categories) and the baseline scale (two categories). Further, as to the value of the Oliver scale in sentencing, Mr Griffiths believes that it is too simplistic to reason that because a person has possession of a lot of images, and the images they have are in the worst categories, they are deserving of a higher penalty. By way of further example, Mr Griffiths spoke of the type of offender who sits at his computer for hours each day collecting large numbers of depraved images but who will never abuse a child himself, compared with an offender who has a small collection of images that resemble the girl next door whom he fantasises about abusing. Acknowledging the difficulty in assessing the risk of contact offending, Mr Griffiths suggests that the period of time over which an offender has had his or her collection, and how the collection was developed, are more relevant to the question of the seriousness of offending, than the number of images in any particular category.

While that point is well made with reference to the risk an offender poses to the community, the significance of the quantity of child exploitation material in the worst categories is often said by courts to be that the actual harm to the children the subject of the material is greater. It is that factor that elevates criminality rather than the indeterminate, or indeterminable, risk that the offender might pose a risk of contact offending.
Suggestions for reform of the classification process were made to the Commission by the CCC and the QPS (as an alternative to the position that there should be no classification beyond whether material is child exploitation material or not). The CCC referred to the recent changes in the classification process in the UK where the categories have been reduce to three:

- Category A – penetrative sexual activity and sexual activity with an animal or sadism
- Category B – non-penetrative sexual activity
- Category C – other indecent images not falling within categories A or B

The CCC recognised that categorising the severity of the images in question is a necessary task for the court to fix appropriate sentences, but maintained that a review of the categorisation system should be considered. In particular, the CCC submitted that strategies should be considered to reduce the workload involved in the current classification process to allow more appropriate prioritisation of policing work.59

The changes in the UK came about after wide consultation by the Sentencing Council with members of the public, judges, magistrates, legal practitioners, police from various districts, non-government organisations (such as Internet Watch Foundation and the National Society for the Prevention of Cruelty to Children), victims, the Crown Prosecution Service, the Law Society and academics. The consultation process was approached with care and was undertaken over a number of years.

Like here, police supported a reduction in the number of categories. The Association of Chief Police Officers National Grading Panel is responsible for producing guidelines for investigators in relation to counting and classifying indecent images of children. While it considered that there should be a maximum of three categories, some expressed the view (shared by police in Taskforce Argos) that that could be reduced to one or two categories.

The UK now employs the new three-category classification tool as the first step in a very prescriptive process informed by the Sexual Offences Definitive Guideline. That Guideline provides ‘offence ranges’ and establishes different categories to reflect varying degrees of seriousness of offending. ‘Category ranges’ define a starting point from which to calculate the appropriate provisional sentence, taking into account aggravating and mitigating features.

The ODPP in Queensland ‘does not support any move away from the categorisation of child exploitation material and maintains that categorisation provides an important objective criterion against which some aspects of criminality can be assessed.’ Acting Director of Public Prosecutions, Michael R. Byrne QC, expressed the view that while the Oliver scale, as it has been adapted in Queensland, is not the only appropriate means of classification, any alternative system should include sufficient specificity to enable a sentencing court to properly undertake a comparison of that aspect of respective criminality.60

The Acting Director of Public Prosecutions does accept, however, as a general proposition, that a review of the categorisation processes should be undertaken.

In its submission to the Commission, the ODPP suggested that consideration be given to adopting a procedure similar to that found in section 289B of the Criminal Procedure Act 1986 (NSW). That section provides for the use of random sampling of seized child exploitation material as evidence of the nature of the material in its entirety.

An ‘authorised classifier’, meaning a police officer who has undertaken classification training conducted by the NSW police force, may conduct an examination of a random sample. The Criminal Procedure Act does not prescribe the nature of the random sample (that is, the size of the sample relative to the entire collection) nor the classification system to be used (for example, the Oliver scale or COPINE). In R v Gavel [2014] NSWCCA 56, for example, 40,852 images had been seized and 8,173 of those formed the random sample reviewed for classification. Classification was performed using the CETS scale.
Evidence of the findings of the ‘authorised classifier’ regarding the nature and content of the random sample is admissible in the form of a certificate, certifying:

- that the authorised classifier conducted an examination of a random sample of the seized material;
- the findings of the authorised classifier as to the nature and content of the random sample.

The certificate is only admissible if the accused (or a legal practitioner representing the accused) has been provided with a reasonable opportunity to view all of the seized material.

The recently enacted Crimes Amendment (Child Pornography and Other Matters) Bill 2015 (Vic), proposes the introduction of random sampling provisions in Victoria. In commending the bill to the House of Representatives, the Attorney-General for the State of Victoria explained the rationale for the proposed change:

Random sample evidence will be particularly useful in cases involving a high volume of child pornography, where thousands of child pornography images would otherwise need to be analysed. This process will allow the material to be analysed in a much shorter time frame. This reform will also reduce the significant occupational health and safety risks associated with viewing large numbers of disturbing images, and will avoid the violation of the child victims through repeated viewing of the material.

Other Australian states and territories (along with the UK, New Zealand or Canada) do not use a random sampling process in the classification of child exploitation material for use by a court, and it is not a process necessarily supported by the QPS.

Mr Griffiths, who is also a mathematician, informed the Commission about potential flaws in the process of random sampling. Mr Griffiths said that he did not disagree entirely with the use of random sampling, but reiterated that he performs image analysis for the purpose of identifying victims, not simply to categorise them for a court. Other officers, however, might benefit from a random sampling process that obviated the need for them to also assess each individual image in order to assign a category within the Oliver, or other applicable scale.61

Mr Griffiths provided an example involving a Western Australian case where random sampling failed to identify any of the 14 out of 300,000 files that were found to contain previously unseen footage of three different girls being abused. Those girls had been abused by the person in possession of the vast collection of child exploitation material. That person had originally been charged with possession of child exploitation material based on the sample of images chosen for the purposes of prosecution (which had not identified the 14 images of his contact offending).

It was only after all images were analysed and the 14 files involving new material were discovered that the offender was charged in relation to the sexual abuse of the three girls and sentenced to a further period of imprisonment.

Mr Griffiths contends that the mathematics applied to choosing a random sample from a given population do not hold true when the categorisation against a nine point scale is applied:

Put simply, the mathematics hold true where one simple (binary) question is asked of each item within the sample, with a ‘Yes’ or ‘No’ answer (for example, is this child exploitation material?). Where the question asked is complex (for example ‘Which of nine distinct categories does this file fall into?’) then the mathematics does not hold true and so the statistical analysis applied to categorisation of a random sample cannot be extrapolated to be true for the entire population with the same degree of confidence.62

Clarification was sought as to whether Mr Griffiths’ view remained the same if considering a six-point scale (like the ‘Oliver’ scale used by Queensland courts). He confirmed that it does.

Further, the random sampling model used in NSW (and proposed in Victoria) seems to leave open avenues for dispute that would require legal representatives, and possibly offenders themselves, to view voluminous
collections of child exploitation material to determine the accuracy of the findings of the ‘authorised classifier’. That seems counter-productive to the aim of streamlining the prosecution process and limiting the number of people viewing the subject child exploitation material.

In respect of the classification of material, the Commission’s position is that the adapted Oliver scale should be maintained. The categorisation of material according to that scale facilitates an objective assessment of the nature of an offender’s collection, taking into account the actual harm perpetrated on the victims of abuse. It also provides a way of comparing one offender against another in order to develop consistent sentences that take into account the principle of parity. It also limits the number of people required to look at images of abuse which is important, not only to reduce the risk of psychological harm to the viewer, but to reduce the trauma to victims who are known to suffer on account of the wide dissemination of the material.

Random sampling might partially resolve the tension between the primary focus of police, on victim identification, and the need for sentencing courts to properly appreciate the nature of child exploitation material offending. Returning to the example used above, in a collection of 10,000 images where 8,000 need not be the subject of analysis for the purpose of identifying potential victims, random sampling, would reduce the number of those files requiring classification according to the adapted Oliver scale.

Any change to the current process of classifying child exploitation material for the purpose of sentencing offenders, including the idea of random sampling, should be the subject of consultation and analysis which is beyond the scope of this Inquiry. The Commission notes the Government’s commitment to re-establishing a Sentencing Advisory Council and commends the issues to that body for further consideration.

**Recommendation**

4.11 The Commission recommends that the Queensland Government proposed Sentencing Advisory Council, once established, as a matter of priority, review the use of the current ‘Oliver scale’ classification system, other classification options, and the merits of using random sampling, in the sentencing process.

**Endnotes**

2. Parliament of Victoria, Hansard, 5 August 2015.
4. *Crimes Act 1958* (Vic), Part II, Division 1, Subdivision (1).
5. Parliament of Victoria, Hansard, 5 August 2015.
Online child sexual offending & child exploitation material

4


Section 3C Crimes Act 1914 (Cth); Section 247A Crimes Act 1958 (Vic).


Section 272 Crime and Corruption Commission Act 2001 (Qld).

Transcript of Interview, Jon Rouse, 2 July 2015, pp. 46–48.


Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth), p. 2.


4.6 Responses to organised crime

4.6.1 Queensland Police Service

The Queensland Police Service (QPS) recognises that organised crime continues to become more pervasive, exploiting existing markets through innovation and adaption, and transgressing into new markets that once would not have been considered organised crime. The QPS also acknowledges that while traditional illicit markets, such as the illicit drug market, continue to be of interest to criminal elements, innovation and adaptability have seen criminal enterprises take advantage of new technologies and opportunities, and expand into areas such as financial crime and child abuse.

The Child Safety and Sexual Crime Group is one of four specialised groups within the State Crime Command. It holds the responsibility for developing and providing a specialist state-wide response to the investigation and management of all types of offending against children. It includes Taskforce Argos, the Child Protection Offender Registry and the Child Trauma and Sexual Crime Unit.

Taskforce Argos is the specialist unit responsible for the investigation of organised paedophilia, child exploitation and computer-facilitated child exploitation. It also holds the Victim Identification Unit, which
Taskforce Argos was established as a multi-disciplinary Taskforce in February 1997 to target organised and serial paedophilia.

Resources

The Commission was provided with information regarding the human resources available to the QPS ‘Child Safety and Sexual Crime Group’. The Detective Superintendent of that group has recently changed. Detective Inspector Jon Rouse is the officer-in-charge of Taskforce Argos, while Paul Griffiths occupies the role of Victim Identification Coordinator.

Like the position taken in respect of the Drug and Serious Crime Group, the position taken by the QPS is that the number and rank of police officers attached to the Child Safety and Sexual Crime Group and Taskforce Argos cannot be published due to operational sensitivities and vulnerabilities. That means that the Commission is not in a position to make any meaningful comment about the adequacy of human resources in this area.

The Commission is able to disclose that Taskforce Argos is comprised of a number of teams, described as follows:

- Social Media
- Mobile Apps
- Adult Chatting
- Peer to Peer
- Darknet
- Operation Commitment.

The Commission had the benefit of information provided by Detective Inspector Jon Rouse and Mr Paul Griffiths in interviews during the course of the Inquiry. It became apparent that Taskforce Argos operates differently than other units within the QPS.

There is urgency in attempting to identify the child victims for obvious reasons, and considerable effort is invested in locating the victims and removing them from harm. Taskforce Argos investigates the crimes committed upon the victims, prepares briefs of evidence against offenders and readies matters for prosecution. However, the ‘front end’ of its operations are squarely in identifying as many child victims as possible from the thousands of images and video recordings that surface on the Internet, and rescuing them from abusive circumstances.

The role of the Victim Identification Coordinator

Mr Griffiths is a civilian employee with Taskforce Argos and has been employed by the QPS since 2009. He is the Victim Identification Coordinator for the unit and is responsible for identifying (and assisting others to identify), where possible, child victims depicted in child exploitation material that comes to the attention of Taskforce Argos. Once identified, efforts are made to locate the victim (whether the child is thought to be in Queensland, or interstate or overseas) and remove him or her from harm.

Mr Griffiths began his career in the area of online child abuse in 1995 with the Greater Manchester Police. His role then was to look for illegal child material in the context of investigating adult obscenity. Mr Griffiths was initially tasked with the identification of offenders who traded the material, but in the process, was able to identify some offenders who produced the material. Once some producers of the material were identified, Mr Griffiths began looking for the victims portrayed in the material. That was in around 1999.
Mr Griffiths worked for the United Kingdom National Crime Squad in a paedophile online investigation team. That team is now known as the Child Exploitation and Online Protection Centre. This Centre is tasked to work both nationally and internationally to bring online child sex offenders, including those who produce, distribute and view child abuse material, before the UK courts. Mr Griffiths remained with the Centre, and headed the Victim Identification Team, until he relocated to Australia in 2008.

Mr Griffiths has been involved with Interpol since 2003, when he became the Chair of the Internet Facilitated Crimes Against Children Group. He also became Chair of the Victim Identification Subgroup. Recently, Mr Griffiths was elected as the overall Chair of the Crimes Against Children Group. The group meets annually and practitioners discuss ongoing trends, problems, solutions and best practices in relation to a variety of crimes against children.  

Mr Griffiths is the only expert of his kind in Australia, and he is arguably the international expert in his field. There is one other person (employed by the Australian Federal Police (AFP) and based in Canberra) who performs this function. There is no other designated victim identification officer in Australia.  

In addition to his victim identification work, Mr Griffiths also provides training in the area of investigations of online child sex offending across the country and overseas.

The Commission agrees with the view expressed by Detective Inspector Rouse that there is a need for Mr Griffiths to have two additional full-time civilian employees working in the Victim Identification Team. The additional resources would ensure that Mr Griffiths has the support his role demands, as well as providing some form of succession planning. 

Other resourcing issues

Taskforce Argos also requires full-time dedicated forensic computer technicians. The Electronic Examination of Evidence Unit employs District Electronic Evidence Technicians, who are deployed across the state to assist with investigations of various types. The Unit is housed in the Fraud and Cyber Crime Group.

Given the nature of the work, it is not unreasonable that Taskforce Argos has dedicated specialist resources such as are available to the Cerberus Unit at the Crime and Corruption Commission (CCC) (see below). Detective Inspector Rouse stated that he requires a minimum of two full-time forensic technicians to be assigned to the unit. The Commission supports the provision of those additional resources.

There also appears to be a resourcing gap in the intelligence capability of Taskforce Argos. Given the reality of finite resources and the prevalence of online child sex offending, intelligence assessments are critical to the appropriate allocation of resources in this area.

Developing a cross-jurisdictional approach to investigating online child sex offending

Detective Inspector Rouse began working in Taskforce Argos in 2000. At that time, the Internet was relatively new to the general public. It facilitated emerging crime types, and the QPS was feeling its way in those early days to determine the threats posed online by child sex offenders.

Although technology was rudimentary and the communications applications available were limited, child sex offenders were visible on some bulletin boards and on the Internet relay chat forum. The networked aspect of child sex offending had already been seen in Europe and other parts of the world, and ultimately a nexus was seen between those international networks and Queensland.

In the years between 2000 and 2004, Taskforce Argos came to better understand the nature and extent of global child pornography distribution networks and the importance of national and transnational cooperation. Two cases involving Taskforce Argos, detailed below, highlight the developments.
Case study

R v D

D was sentenced in 2003 and is currently serving an indefinite sentence for sexual offending against more than 60 children (some as young as 12 months old) over a period of almost 28 years.

The offending came to light by accident when D left a video camera for repair and a video containing some of the 500 hours of footage was ultimately found. D had abused his younger sister and his own daughter, and had gained access to other children through friends and family, and by obtaining positions as a church leader and gymnastics instructor.

It was only discovered that D had been distributing still images of his abuse of children after his sentence, when French police asked Detective Rouse to look at some images connected with the arrest of an ex-Tasmanian police officer, called H. H had recently been arrested by the QPS.

The images that the French authorities were interested in were also in the possession of Interpol, and were the subject of victim identification investigations. Officers of Taskforce Argos were able to tell international authorities that the children who were the subject of D’s images were now safe on account of his arrest and incarceration.

By 2004, Taskforce Argos had been involved in a number of international investigations, and positive international relations had been established. A significant number of operations had also been completed in Queensland.

Operation Falcon, in 2004, presented the next learning curve. The investigations involved the use of credit cards to access pay-per-view websites. Targets were sent from the United States, and the operation resulted in 700 search warrants being executed across the Australian states—with 128 Queensland residents being targeted. Ultimately, 80 Queensland offenders were arrested.

Queensland had the third largest target list, following New South Wales and Victoria, but was the only state to identify victims. No other state looked for contact offences in the material it seized from offenders, and no other state took into account that the offenders might produce their own material and share it. Detective Inspector Rouse saw this as a failure of the operation, and decided that a victim image database was needed. He raised the issue at the 2005 conference for Police Commissioners, and the move for the database was supported. A national database called the Australian National Victim Image Library (ANVIL) was developed.

Around the same time, the AFP developed capability in the field of online child sex offending, and Commonwealth legislation was amended. That was just in time for the online child sex offending landscape to change again.

As described below, operation Achilles commenced in 2006 and targeted a new level of networked offending.
Case study

Operation Achilles

This operation commenced in January 2006, after the QPS received information from officers in New Zealand when an offender disclosed passwords and access codes to an international paedophile network of which he was a member. The network dealt with child exploitation material, which included financing the production of movies-on-demand depicting the violent sexual abuse of children.

The group had operated for fifteen years, and administrators of the group used encryption of operating systems as well as other techniques to hide their activities—including firewalls, port scanning, proxies and anonymising services that remove the ability for the IP to be tracked. The administrators also developed software that allowed movie files to be split into segments, with the order of the segments being altered. This resulted in the movie file being unable to be played unless a member employed the de-encryption process required.

To gain membership to the group, a prospective candidate was tested on image recognition of his or her own collection of child exploitation material. The group administrators developed a software application that was sent to the prospective member, which allowed an analysis of the person’s hard file and image contents. The prospective member was then asked for specific details of images in the collection. This would prove to the group that the prospective member was not a law enforcement agent, as agents were barred from distributing child exploitation material. This also allowed the administrators to glimpse the extent of the image collection of the prospective member.

Later, it became known that members included offenders from the United States, Germany, Austria, the United Kingdom and Australia.

Taskforce Argos took over the investigation from New Zealand police, and officers interviewed the offender, which allowed Queensland police to take over the identity of the offender and infiltrate the network.

This was the first big step by Taskforce Argos officers into a large sophisticated network. The operation continued over three years. The involvement of the United States Federal Bureau of Investigation (FBI) in the investigation came about because the anonymising servers of the group were hosted in the United States. The FBI sent an agent to Brisbane to work with Taskforce Argos officers. Following this initial collaboration between the FBI and the QPS, operational efficiencies resulted in an officer from Taskforce Argos being sent to the United States to assist in the investigation. This officer spent 18 months with the FBI in the United States, working collaboratively with Taskforce Argos officers to assist in the identification of victims.

Other international law enforcement agencies also became involved in the investigation as it progressed. These included the United Kingdom’s Child Exploitation and Online Protection Centre, Interpol France, and the German Federal Criminal Police Office.

Within the course of the investigation, over 500,000 communications within the group were analysed. Ultimately, 14 United States offenders, four German offenders, two UK offenders and two Australians were identified and arrested. The largest seizure of electronic data in the history of the United States was made, consisting of 58 terabytes of material. The operation closed on 29 February 2008.

Operation Koala was a further investigation resulting from Operation Achilles, and resulted in hundreds of arrests globally. As a consequence of both operations, more than 60 children were removed from harm around the world, an Italian administrator of a child exploitation website who also produced material was arrested, and four commercial websites dealing in child exploitation material were shut down.

The contribution of Taskforce Argos to this investigation—on a global scale—was enormous, and demonstrates the expertise and collaboration it brings to the world-wide fight against online child sex offending.
Cross-jurisdictional initiatives

Detective Inspector Rouse learned early on in his time with Taskforce Argos the significance and importance of forging positive relationships with international law enforcement agencies. This realisation, and his dedication to maintaining these relationships, have resulted in many children being identified as victims of sex offences.

As international relationships were forged through the experience with French police in relation to ‘D’ and ‘H’ in the R v D case study above, and through operations like Falcon and Achilles, it became obvious to Detective Inspector Rouse that some form of library or database of images was required.

The meeting with the French police officer also led Detective Inspector Rouse to use an application that allowed Taskforce Argos to share material it was uncovering with international law enforcement agencies. These agencies included Interpol, the Swedish National Police, and the German Federal Criminal Police Office, as well as agencies from the United Kingdom, Norway, Switzerland, Toronto and others. The application allowed any law enforcement agency to post discovered images online, and all other agencies could immediately see the images and assist in the search for the child victim. It acted as a virtual office space and ran 24 hours a day, seven days a week. It also allowed for instant messaging between agencies and the sharing of information. The software is still used by Taskforce Argos officers.

Taskforce Argos also makes good use of a number of databases, including the database held in the United States by the law enforcement agency, National Centre for Missing and Exploited Children (NCMEC). The other database used is the International Child Sexual Exploitation Image database (ICSE) held by Interpol.

Taskforce Argos takes steps necessary to have images uploaded to the ICSE database. The sharing of information relating to child exploitation material with national and international law enforcement agencies is important for a number of reasons. First, in the United States, a prosecution for child exploitation material can only proceed if the child depicted in the image is identified, even if the child is identified as an Australian child or from elsewhere in the world. The uploading of images alerts all participating law enforcement agencies to the identity of the investigating officer and whether an offender or child victim has been identified.

Second, sometimes a law enforcement agency in another country comes across one or more images of an Australian child, identifiable by some feature unique to Australia (for example, registration plates or identifiable places of interest). That information can lead to the identification and rescue of that child.

Third, images may surface overseas that provide evidence of an offender in Australia having committed contact offences with children. It may be that when an offender in Queensland is charged with child exploitation material offences, the hard drives of the offender are encrypted. The offender may only be dealt with for possession of child exploitation material. However, the offender may have previously uploaded images which depict him or her sexually offending against a child, and it is these images that have come into the collections of databases held by other countries.13

The fact that Taskforce Argos officers routinely upload images to the database held by Interpol means that there is regular contact and collaboration with law enforcement agencies all around the world. This collaboration is strong and productive. It places Taskforce Argos firmly in the position as one of the world leaders in the investigation of online child sex offenders.

The international cooperation between Taskforce Argos and other law enforcement agencies is not formalised in the sense of memoranda of understanding or other formal agreements.14 Detective Inspector Rouse was asked by the Commission if he considered the informal nature of the relationships sufficient to cover any future change in personnel, either within Taskforce Argos or in the international arena. Detective Inspector Rouse considered it would be a difficult task to undertake to put any formal agreements in place. However, he is very aware of the potential issues associated with succession and the need to forge international relationships that would weather a change in personnel.
To that end, Detective Inspector Rouse has implemented a number of steps. For example, three years ago, he organised a Queensland-based conference of law enforcement agencies, allowing officers attached to Taskforce Argos to make connections with international personnel. This conference now occurs annually, so that there is an ongoing opportunity for all officers to make new—or maintain existing—connections.

Further, for the past three years, two investigators from Taskforce Argos have attended the Crimes Against Children Conference, held annually in Dallas, Texas. This conference is internationally recognised as the premier conference of its kind, providing practical and interactive instruction to those fighting crimes against children and helping children heal. This has allowed officers coming up through the ranks in Taskforce Argos to meet—and begin to make their own connections with—personnel from law enforcement agencies across the world.

Detective Inspector Rouse has also ensured that, for the past two years, a Taskforce Argos investigator attends a training course conducted annually in Selim, Germany, called the Europol Training Course on Combating the Sexual Exploitation of Children on the Internet. He is in the process of negotiating for an officer to attend this year’s course. The participation by a Taskforce Argos investigator in this forum also ensures that international relationships are forged.

Mr Griffiths’ role as a Chair for an the Interpol group, Crimes Against Children Group, further cements Taskforce Argos in the international law enforcement environment.

**Referrals by Australian law enforcement agencies**

The Commission was told of the QPS procedures in place to ensure the dissemination of information relevant to national and international investigations to the various law enforcement agencies. Taskforce Argos has established a standardised process for the dissemination of investigations and intelligence reports with national and international law enforcement agencies to ensure timely, consistent and relevant action. When an information or intelligence package—including all electronic evidence (images/videos or screen captures), statements and any other supporting material—is developed by a referring jurisdiction, consideration is given to any specific evidentiary requirements that might exist in the receiving jurisdiction.

Once the evidence package has been sent to the relevant jurisdiction, the referring jurisdiction will communicate with the receiving jurisdiction to advise that the package has been sent, and to confirm that it has been received. Taskforce Argos is involved in both the referral and receipt of packages domestically and internationally. Where a domestic referral has been made electronically, a formal written referral is to be sent to the receiving jurisdiction. Where a child at risk has been identified, immediate action is taken to ensure the information or intelligence package is sent to the relevant jurisdiction.

The Australian Federal Police (AFP) will generally facilitate the dissemination of information and intelligence packages to international law enforcement agencies. However, there are occasions when the relevant state or territory law enforcement agency has already an established network or relationship with the particular international agency. In that case, the protocol requires the AFP to be advised of the dissemination that has already been facilitated by the state agency.

In cases of urgency involving child protection, a secure electronic platform is used to send information or intelligence to the international agency by the relevant state agency. The AFP is kept informed of this situation. If the relevant international agency does not have a secure electronic platform in place, the referral of the package will be made either through the AFP, Interpol or Europol.

The fact that Taskforce Argos investigators are able to secure the rescue of children internationally within 12 to 36 hours of the dissemination of information to international law enforcement agencies indicates that inter-agency cooperation at the international level, insofar as this aspect of organised crime is concerned, is commendable.
National initiatives

**JACET (Joint Anti Child Exploitation Team)**

JACET is a joint taskforce between the AFP and various state and territory police forces. Its objective is to accelerate dissemination of information received from international agencies to partner agencies regarding sexual predators who prey on children in the online environment.

In its submission to the Commission, the QPS stated that in April 2015, agreement was reached between the QPS and the AFP for AFP investigators to be co-located within Taskforce Argos to form the Queensland arm of the JACET. Similar teams have been established in most other Australian jurisdictions. Victoria was the first state to sign the memorandum of understanding about JACET, which occurred in October 2014. Western Australia followed suit in December 2014, with South Australia implementing JACET in January 2015. Northern Territory appeared to also incorporate JACET around the same time. New South Wales signed the memorandum of understanding in May 2015.

The establishment of JACET is expected to result in greater cross-agency collaboration, greater access to—and sharing of—information, and more targeted operations across borders.\(^\text{21}\)

The Commission learned that JACET is expected to be implemented in Queensland in the near future.\(^\text{22}\)

There will be a team comprised of AFP officers assigned to Queensland, and they will be physically located in the offices of Taskforce Argos. It is likely that the team will comprise of a senior officer and investigators. A forensic technician might also form part of the team.\(^\text{23}\)

At the time of writing, the JACET Memorandum of Understanding between the QPS and the AFP was in the hands of the Superintendent of Child Safety and Sexual Crimes Group.

---

**Recommendation**

4.12 The Commission recommends that the Queensland Police Service seek to execute and implement, as a matter of priority, the Joint Anti-Child Exploitation Team Memorandum of Understanding.

---

**Kent Internet Risk Assessment Tool**

Mr Griffiths referred to the Kent Internet Risk Assessment Tool (KIRAT) used in the UK and in some parts of Europe to prioritise investigations and assess the risk of an offender also being—or becoming—a contact offender. KIRAT allows police to target known offenders and suspects by pooling information about them and their activities. It was trialled in the UK between 2009 and 2011, after which it was rolled out to 38 police forces. The European Commission provided 1.1 million pounds to help force the roll out in Estonia, Spain and Rotterdam. The Commission was told that KIRAT is being introduced into law enforcement agencies in Australia.

Given what the Commission learned about the volume of known online child exploitation material offenders operating in the south-eastern region of Queensland alone, a tool for effective prioritisation based on risk, such as KIRAT, is considered essential. In addition to skills and resources already available to the QPS and CCC, KIRAT would assist in directing resources to those offenders who are identified as posing the greatest risk of contact offending.
4.6.2 Crime and Corruption Commission

The role and functions of the CCC are set out in some detail in the chapter on illicit drugs, above.

One of the purposes of the CCC is to combat and reduce the incidence of major crime, including ‘criminal paedophilia’.

The CCC aims to fulfil its role in combatting and reducing the diverse and target-rich criminal paedophilia market by working closely with other law enforcement and prosecution agencies including Taskforce Argos and the State and Commonwealth Directors of Public Prosecutions. It recognises the importance of using its specialist resources to target Internet-based offending, repeat offenders and paedophile networks.24

The Cerberus Unit (Cerberus) is the specialist unit tasked with investigating criminal paedophilia within the terms of a General Referral made under Chapter 6, Division 2 of the Crime and Corruption Act 2001. That General Referral was most recently amended in June 2015 to combine the scope of two earlier referrals.

Cerberus is staffed by experienced police officers, forensic computing experts and an intelligence analyst. It also has the support of legal and administrative staff.

The CCC told the Commission that Cerberus is conscious of the need to avoid duplication of law enforcement energies, and it directs its efforts to:

- using covert investigative strategies where appropriate to build strong briefs of evidence
- using its coercive hearings power either to progress its own investigations or to support the QPS investigations
- prioritising investigations and taking action in cases that involve a risk of contact offending
- proactively examining various platforms and software to identify child sex offenders representing the highest threat of harm to children.25

Essentially, the investigative work undertaken by Cerberus is focused on the aspect of the online child exploitation material market using peer-to-peer networking to share files. The CCC told the Commission that wherever possible, the focus will be directed to offenders who are engaging in aggravated (‘networked’) offending within the definition of section 474.24A of the Commonwealth Criminal Code, discussed in detail in the section on the child exploitation market, above.26

Cerberus self-generates targets for investigation by identifying individuals for further investigation without an initial complaint. Further, the CCC differs from the QPS in that it does not directly receive referrals from other law enforcement agencies for further investigation (although it will refer matters to the appropriate jurisdiction when necessary).27 All such referrals from national and international law enforcement agencies are received by Taskforce Argos, which may then pass a referral onto the CCC.

The CCC also provides support to the QPS in high-priority Taskforce Argos investigations, by collecting and examining computer forensic evidence using its specialist resources. That assistance is one aspect of a broader joint agency agreement, which is said to enable the best use of resources by both agencies in the investigation of priority child sex offender matters.28
The Joint Agency Agreement commenced on 12 February 2015. It contemplates mutual cooperation to properly fulfill their respective functions and calls for assistance in various circumstances. The CCC also agrees, under the Agreement, to provide operational assistance to the QPS upon request. That assistance might include:

- the potential use of the coercive powers under the CCA
- forensic computing specialist support
- research resources for projects relevant to strategic questions or themes.

The Agreement also provides for the formation of joint operations.

The relationship between Cerberus and Taskforce Argos

The Commission was told that the Cerberus team has a good relationship with Taskforce Argos and conducts joint investigations with it from time to time. Cerberus performs its own victim identification work; however, since Paul Griffiths is known to be the national expert in victim identification, officers from the Cerberus Team will ask him for assistance as required.

Detective Burke told the Commission that the two units complement each other with their specific strengths and there was no competition over targets. The nature of the software used by both teams means that each unit can identify if the other unit is looking at the same offender.

As to the differences between the two units, Detective Burke told the Commission that Cerberus has a far greater forensic capacity than does Taskforce Argos. Taskforce Argos has ‘sheer numbers’ to cater for a very wide response to the problem of online child sex offending, whereas Cerberus remains focused on generating targets and commencing prosecutions.

From the perspective of Taskforce Argos, the Cerberus Team performs one of the same roles that it performs in targeting offending on peer-to-peer platforms.

Taskforce Argos sees the real value of Cerberus as lying in the capability to conduct coercive hearings and in providing forensic technical expertise. Further, successful joint specialist operations have been conducted in the past (for example, Operation Lima Rhodes leading to the arrest of Shannon McCoole and others).

Statistics

The Commission was informed that over a period of 13 years, Cerberus has arrested 193 people and charged them with 2,825 charges. Of the total number of charges laid, 344 were against Queensland offenders. Some charges were as a result of joint operations with Taskforce Argos.

Detective Senior Sergeant Burke told the Commission that the team averages 12 arrests each year. He said this corresponded to an arrest of one person every four weeks, to allow for the forensic component of the investigation to take place. In a similar sentiment as that conveyed by Detective Inspective Rouse, Detective Senior Sergeant Burke conceded that those arrests barely scratch the surface of known offending. It was pointed out, however, that one offender is typically arrested every second operation for contact offences committed against children. In that sense, some high-priority targets are being caught by investigations.

Like Taskforce Argos, Cerberus uses the software available to attempt to identify the targets representing the highest risk to children. This approach, however, does not account for offenders who have hidden their activities by using encryption or other methods, or offenders who are operating within the Darknet.

Detective Burke told the Commission that Cerberus could generate enough information to justify many more search warrants; however, the forensic effort in mounting each case would create a bottleneck.

Detective Burke was referring to the fact that the QPS has a centralised forensic team that serves the needs of an entire state. He told the Commission that his team does not have that problem, on account of the way they approached the work.
While the Commission accepts the inherent problem in the vast supply of offenders against the scant supply of resources, it is unacceptable that such an enormous group of networked child exploitation material offenders be allowed to continue to offend, largely unchecked by law enforcement. It is recognised that Cerberus and Taskforce Argos do their best with the resources available, but more must be done to tackle what is a relatively easily identifiable market in child exploitation material operating in a networked way (however loosely) in Queensland.

**Recommendation**

4.14 The Commission recommends that the Queensland Police Service and Crime and Corruption Commission be properly resourced, including with technical staff and analysts, to undertake a ‘blitz’ and tackle to a greater degree known Queensland-based offenders sharing child exploitation material on peer-to-peer platforms.

---

**4.6.3 Office of the Director of Public Prosecutions**

The role of the Director of Public Prosecutions and his or her staff in prosecuting people charged with criminal offences, assisting victims, and in restraining and confiscating proceeds of crime, has been dealt with in the chapter on illicit drug use, above.

In respect of online child sex offending, including the child exploitation material market, this chapter has also raised the issue of the wellbeing of staff who are required to view child exploitation material (see the section titled Child exploitation market, above). Staff of the Office of the Director of Public Prosecutions (ODPP) who prosecute or assist in the prosecution of child exploitation material cases are required to view disturbing material from time to time, and the Commission has recommended that appropriate measures be put in place to minimise the risk of harm to those staff.

Further, the Commission learned that Taskforce Argos has a close working relationship with staff in the Commonwealth DPP (CDPP), probably due to the fact that staff within the Human Exploitation and Border Protection Group at the CDPP regularly prosecute their matters. Staff within CDPP regularly prosecute their matters.34

While it is not suggested that the Queensland ODPP ought necessarily restructure its operations to facilitate a dedicated team of prosecutors for child exploitation material matters, Taskforce Argos perceived that it has a role to play in training ODPP staff in the special features of child exploitation material offending that comes to it for prosecution.

Having had the benefit of a number of presentations by Taskforce Argos, the Commission commends that suggestion to the Queensland ODPP.

---

(Endnotes)

3 Transcript of Interview, Jon Rouse, 2 July 2015; Transcript of Interview, Jon Rouse, 18 August 2015; Transcript of Interview, Paul Griffiths, 24 July 2015.
4 Transcript of Interview, Paul Griffiths, 24 July 2015, p. 4.
<table>
<thead>
<tr>
<th></th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Transcript of Interview, Paul Griffiths, 24 July 2015, p. 11.</td>
</tr>
<tr>
<td>6</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 29.</td>
</tr>
<tr>
<td>7</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, pp. 29, 32, Transcript of Interview, Jon Rouse, 18 August 2015, p. 22.</td>
</tr>
<tr>
<td>8</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 32.</td>
</tr>
<tr>
<td>9</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 33.</td>
</tr>
<tr>
<td>11</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 2.</td>
</tr>
<tr>
<td>13</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, pp. 2–4.</td>
</tr>
<tr>
<td>14</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 8.</td>
</tr>
<tr>
<td>16</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 21.</td>
</tr>
<tr>
<td>18</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 45; Transcript of Interview, Jon Rouse, 18 August 2015, p. 22.</td>
</tr>
<tr>
<td>20</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, p. 7.</td>
</tr>
<tr>
<td>22</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, pp. 32–33.</td>
</tr>
<tr>
<td>23</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, pp. 32–33.</td>
</tr>
<tr>
<td>27</td>
<td>Transcript of Interview, Cameron Burke, 23 July 2015, pp. 8, 9, 51.</td>
</tr>
<tr>
<td>30</td>
<td>Transcript of Interview, Cameron Burke, 23 July 2015 (2957365), pp. 9, 51.</td>
</tr>
<tr>
<td>31</td>
<td>Transcript of Interview, Jon Rouse, 2 July 2015, pp. 48–50.</td>
</tr>
<tr>
<td>34</td>
<td>Affidavit of David Norman Adsett, 31 August 2015, paras 4–11.</td>
</tr>
</tbody>
</table>
4.7 Future trends and emerging markets

The Australian Crime Commission’s Organised Crime Threat Assessment (OCTA) identifies the key nationally significant organised crime threats, to allow for an integrated and collaborative Commonwealth response to organised crime.¹

OCTA is a market-based assessment that provides a strategic overview of the dynamics within each key illicit market operating in Australia, including child sex offences. OCTA provides risk ratings and an assessment of the degree to which serious and organised crime is involved in those markets.²

Consistent with Europol’s assessment of the changing nature of organised crime, the 2012 OCTA noted the emergence of the entrepreneurial individual as a key player in a number of significant illicit markets. In 2014, OCTA noted:³

This phenomenon, enabled by globalisation and technology, and observed internationally, has necessitated a shift in the way in which the threat can, and should, be contextualised. Significant harms can now be wrought by actors who operate outside traditional organised crime structures to commit serious crime.

Although organised crime groups remain active in Australia and internationally, particularly in the traditional drug markets, the broader threat picture has a variety of actors. For this reason, the threat in OCTA 2014 is characterised as the threat from serious and organised crime, rather than from organised crime groups.

On the basis of the information received by the Commission from a range of law enforcement and intelligence sources, there can be little doubt that child sex offending, particularly to feed the illicit and insatiable child exploitation material market, represents a risk with an upward trajectory.

Further, there is a growing trend towards commercialisation of the child exploitation material market. Despite the fact that child exploitation material is often viewed as the commodity in itself, the Queensland Police Service (QPS) told the Commission that offenders are increasingly using difficult-to-trace crypto-currencies to purchase or obtain access to child exploitation material.⁴ Mr Griffiths told the Commission that he had seen an increase in the commercialisation of material by way of more requests for production of material on demand with payment required—by Bitcoin, Western Union transfers or even Paypal.⁵ The case study involving the offender Rivo in the section titled Online child sexual offending, above, is a good example. The use of remitters and virtual currencies is addressed in more detail in the chapter on financial crimes.

As previously mentioned, Detective Inspector Jon Rouse of Taskforce Argos described networking amongst sexual offenders as evolving rather than emerging.⁶ He stated that as technology changes, offenders and their networks evolve and use new technology to add depth to their offending and to avoid detection. Those sentiments were echoed by civilian expert Mr Paul Griffiths.⁷

Detective Rouse told the Commission that sex offenders have, for some time, been known to form networks. By way of example, he referred to the arrest of an offender many years ago, who had operated a child sex offenders’ network via CB radio. That network boasted a membership of about 170 offenders.⁸

The network of more than 45,000 members, administered by Shannon McCoole using Tor on the Darknet, shows the extent to which technology and the cyber environment has enabled the growth of global, sophisticated networks of child sex offenders. That growth is likely to continue with ongoing advancements in technology.
A 2011 longitudinal study further demonstrates the growth trend. The study, conducted in 2000 and then again in 2006, found growing numbers of offenders with larger collections and an increased propensity to share child exploitation material (abbreviated as ‘CEM’ in the table below).9

<table>
<thead>
<tr>
<th></th>
<th>2000</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of sample using P2P networks to access and trade images</td>
<td>4%</td>
<td>28%</td>
</tr>
<tr>
<td>Percentage of offenders arrested for possession of CEM who identified as having distributed CEM</td>
<td>33%</td>
<td>39%</td>
</tr>
<tr>
<td>Percentage of offenders with-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>more than 1,000 CEM images; and</td>
<td>14%</td>
<td>20%</td>
</tr>
<tr>
<td>more than 50 videos</td>
<td>8%</td>
<td>16%</td>
</tr>
</tbody>
</table>

Offenders who used peer-to-peer networks were also identified as having the most graphic material which typically included children under three years old and had elements of bestiality, sadism or torture.

Although nearly a decade old, this study highlights that not only is the quantity of child exploitation material collected by offenders increasing, it appears more people are sharing it and the content is becoming increasingly sadistic and graphic.

The findings of this study accord with information provided by Mr Griffiths, who told the Commission that offenders in Queensland are seeking out images and videos of younger and younger children, with many images of babies being offended against made available for viewing. Mr Griffiths was aware of two cases where offenders planned the abuse of children even before they were born, and took requests from offenders for the production of child exploitation material.10 Another emerging trend, which has been seen for several years, is the demand for more ‘hard core’ and ‘hurt core’ images and videos.

Predators will also continue to use whatever platforms available to groom and procure children, including on social media, in online chat rooms, and using online gaming platforms (such as Xbox Live, Playstation Network and the PC online gaming network running through platforms such as Steam).

The United States Federal Bureau of Investigation (FBI) issued a warning to parents as far back as 2011, saying that paedophiles go wherever children are. Before the Internet, that meant playgrounds and amusement parks, whereas the virtual world makes it alarmingly simple for predators, who pretend to be children themselves. Executive Assistant Director at the FBI, Shawn Henry, issued this advice:11

Parents need to talk to their children about these issues…. It’s no longer enough to keep computers in an open area of the house so they can be monitored. The same thing needs to be done with online gaming platforms.

Further, research undertaken by Professor Julia Davidson in the UK found that offenders were branching out into gaming platforms in order to target young people, particularly boys. Conversations between predators and children online were seen to become sexualised within a matter of minutes, with some offenders reporting that they no longer needed to bother with grooming children when they could immediately ask for sex, or to meet to facilitate sexual abuse. Researchers found that some offenders spent up to six hours a day on ‘fishing expeditions’ where they pepper hundreds of children until they find one willing to interact.12

The QPS supports national awareness campaigns such as the Australian Federal Police Think U Know campaign. It has also promoted campaigns such as Your Selfies, Keep It To Yourself, Who’s Chatting To Your Kids and Surf Safely through schools and online in order to assist children and their parents to maintain safe
In the YouTube video promoting the first-mentioned program, Detective Rouse emphasises that education will be the most critical tool in protecting children in the online environment.

There is a raft of online educational material supporting all of the programs, including information aimed to raise awareness among parents, carers and teachers ‘of how young people are using technology, the challenges they may face and how to help them navigate these challenges in a safe and ethical way.’ The topics include privacy management, online grooming, sexting and inappropriate content. Further information about the techniques used by predators is available to parents and caregivers though the QPS’s Who’s Chatting to Your Kids campaign.

Online safety tips in the QPS Surf Safely campaign reminds young people that predators will ask personal questions in an attempt to become friends quickly, and can use personal information to find them online. Warnings are issued against accepting invitations to view webcams from strangers and arranging face-to-face meetings.

The Australian Curriculum ‘sets consistent national standards to improve learning outcomes for all young Australians.’ Insofar as cyber-safety is concerned, the Australian Curriculum provides:

- Identifying and managing risk in Technologies learning addresses the safe use of technologies as well as risks that can impact on project timelines. It covers all necessary aspects of health, safety and injury prevention and, in any technologies context, the use of potentially dangerous materials, tools and equipment. It includes ergonomics, safety including cyber safety, data security, and ethical and legal considerations when communicating and collaborating online.

... When state and territory curriculum authorities integrate the Australian Curriculum into local courses, they will include more specific advice on safety.

The Queensland Department of Education, Training and Employment has produced a number of guides and aides for teachers and parents in respect of cyber safety and cyber bullying. The Commission was also made aware of various aides for teachers and caregivers which cater to different age groups.

Another recent federal government initiative is the establishment of the Office of the Children’s eSafety Commissioner. The Office is said to lead online safety education for the Australian Government and protects children when they experience cyberbullying, by administering a complaints scheme. The Office’s role is focused on cyberbullying; however, eSafety information available on the website includes advice about unwanted contact, sexting and protecting personal information and privacy while online gaming.

Given the ingenuity and relentlessness of online predators, and the ever-increasing appetite for new and depraved material in the child exploitation material market, those education initiatives must continue to be properly funded and delivered in a robust way by providers. The threat to children from online predators is very real, and is growing in magnitude and volume. The importance of impressing that message upon young people in an appropriate way cannot be overstated.
### Endnotes


6. Transcript of Interview, Jon Rouse, 2 July 2015, p. 28.

7. Transcript of Interview, Paul Griffiths, 24 July 2015, p. 11.

8. Transcript of Interview, Jon Rouse, 2 July 2015, p. 28.


5.1 Introduction

It is well-documented that financial crimes are a significant part of the organised crime landscape. Financial crimes are diverse in nature and scale, as well as in respect of the level of harm they cause.\(^1\) They ‘encompass a range of illicit activities including fraud, money laundering, terrorist financing, white collar or corporate crime, proceeds of crime, bribery, currency violations, financial market offences, tax evasion, and cyber and technology-enabled crimes relating to financial activity.’\(^2\)

Financial crimes are committed not only as a means to an end (for example, to launder money made from other illicit activity), but also as a direct means of making profit.

Like in other areas of organised crime, sophisticated technology and global markets have provided new opportunities for organised crime syndicates. Criminal enterprises committing financial crimes are increasingly transnational and complex—often using legal business structures and intermingling licit financial transactions with the illicit to make detection and prosecution more difficult. To add to the challenge, these types of crimes are notoriously under-reported for a range of reasons, including the shame victims feel in being duped, and the need to protect reputation for corporate victims.

According to the Australian Crime Commission (ACC):

[T]he risk posed by financial crime is particularly salient in the current economic environment, in which damage to financial markets, financial institutions, government revenue bases and savings by private individuals can have far-reaching implications for the economic recovery of nations.\(^3\)

Significantly, investment and financial market fraud is identified by the ACC as a significant risk to Australian individuals and organisations. The risk has seen a marked increase since 2012.\(^4\)

The Terms of Reference required the Commission to focus on financial crime as a ‘key area’, paying particular attention to investment and financial market fraud, and financial data theft. This chapter deals with those areas of focus—along with key enablers such as identity theft, cyber and technology-enabled crime, and professional facilitators. Money laundering is dealt with separately in the following chapter.

Insofar as investment and financial market fraud is concerned, inquiries focused the attention of the Commission on fraudulent investment schemes, in the form of cold-call investment frauds commonly known as ‘boiler-rooms.’\(^5\)

The Commission learned that, while boiler-room operations have traditionally been seen as operating for the most part offshore, the Gold Coast now appears to be a hub of onshore boiler-rooms. This is a problem that has been known to the...
Financial Crimes

Queensland Police Service (QPS) for some years, but despite that, the issue has not been prioritised nor has the QPS been resourced sufficiently to deal with it.

These fraudulent cold-call investment schemes are undoubtedly a form of organised crime, using professional facilitators (for example, accountants and IT experts), sophisticated and complex business structures, and aggressive telemarketing campaigns to defraud victims of millions of dollars.

The extent and nature of cold-call investment frauds and other types of investment and financial market fraud are detailed in the following section. That part also addresses the economic and societal impact of those types of organised financial crimes, as best as can be known, given the paucity of data.

Other types of crimes typically considered by law enforcement and intelligence agencies in the category of investment and financial market fraud include:

- manipulation or exploitation of the legitimate share market to artificially raise or lower the price of securities for financial benefit—for example, ‘share ramping’ or ‘pump and dump’ schemes
- exploitation of financial securities to commit fraud or launder or conceal the proceeds of crime—for example, off-market share transfers and fraudulent share schemes.

Financial data theft is addressed in the section by that title. For the purpose of this report, that term includes activities that are often described as ‘crimes in the mainstream economy’, as well as other less-traditional—but increasingly common—methods of financial data theft, such as:

- card—including card-not-present—fraud
- skimming and counterfeit cards
- phishing, vishing, spear-phishing
- malware and ransomware
- hacking, pharming and keylogging
- mail theft
- advance-fee fraud and spam emails
- romance/social networking scams

Enabling activities are detailed in the section titled Related activities, below. All of the key enablers articulated in the Terms of Reference, are relevant to the success of organised financial crime. For example:

- Cyber and technology-enabled crime: facilitates global enterprises and transnational structures, as well as allowing for anonymity through the use of technologies such as Voice Over Internet Protocol (VOIP) and virtual currencies.
- Identity crime: said to be arguably the fastest growing crime internationally, causing staggering financial losses and facilitating other crimes such as drug trafficking, people smuggling and money laundering.
- Extortion: ransomware, a form of hacking, used to extort money from governments, business and individuals by attacking computer systems and threatening data.
- Professional facilitators: participate wittingly and unwittingly in organised financial crime by, for example, establishing complex business structures and developing websites.

The legislative framework and perceived gaps and inadequacies are addressed in the section titled Legislation, below. Upon analysis of maximum penalties and the range of offences available in other states to deal with the diverse range of financial crimes, amendments to the Criminal Code are recommended. The Commission also considered concerns raised by law enforcement officers about obtaining bank records in a timely manner. Recommendations are made with a view to addressing that perceived vulnerability.

The adequacy and appropriateness of the current responses of Queensland law enforcement, intelligence, and prosecution agencies to prevent and combat organised crime in the area of financial crimes is dealt with in the section titled Responses to organised financial crime.
Significantly, that part of the report addresses the perceived failure of the QPS to adequately respond to the serious and ongoing problem of boiler-room frauds now flourishing on the Gold Coast. The scale of the organised crime problem is vast and, to date, inadequate resources have been directed to combatting it—whether by means of prevention, disruption or investigation. The Crime and Corruption Commission has played an important role in making some progress; however, it is the view of this Commission that more must be done as a matter of priority.

This chapter, in the section on future trends and emerging markets, identifies a number of growing trends. Among them, law enforcement has recently seen some evidence of foreign trading fraud in Australia, particularly using online trading platforms. Given the size of the global foreign exchange market, the volume of transactions, the lack of regulation and the volatility of the market, investment fraud syndicates are likely to see the foreign exchange market as a vehicle for defrauding investors globally. The use of virtual currencies—such as Bitcoin—and the alarming incidence of extortion by the use of ransomware is also discussed.

(Endnotes)

5 The terms cold-call investment fraud and boiler room fraud are used interchangeably in this report.

5.2 Investment and financial market fraud

Investment and financial market fraud is identified by the Australian Crime Commission (ACC) as a significant risk to Australian individuals and organisations.

Financial market fraud is increasingly committed by organised crime groups, with ‘the opacity of the beneficial ownership of Australian-shares’, providing opportunities for organised crime entities to hide their involvement in illicit activities through, for example, money-laundering and tax evasion. The foreign exchange market is also seen as an attractive platform for defrauding investors globally.

The ACC additionally warns that organised crime involvement in superannuation fraud in Australia is more significant than was previously thought. In particular:

  The focus of the threat has shifted from opportunistic individuals to well-resourced and sophisticated international organised fraud networks actively targeting the Australian Superannuation sector.

The pool of compulsory superannuation savings in Australia is estimated to be worth $1.62 trillion, making it a very attractive target for organised crime. Self-managed funds are particularly vulnerable, with some inexperienced investors susceptible to fraudulent investment pitches.
Investment fraud is a type of organised crime that the Commission found to be rife in Queensland. Many Queensland residents have lost combined millions to fraud, perpetrated by offenders located here, as well as interstate and overseas. The Commission’s attention was focused on a type of ‘Ponzi’ scheme known as cold-call investment frauds, or boiler-rooms. This focus was brought about by the discovery of a burgeoning problem involving that type of organised crime on the Gold Coast.

This section of the report outlines some common modus operandi of fraudulent cold-call investment schemes, including sports arbitrage and stock market prediction software scams. The nature, prevalence, and economic and societal impacts of cold-call investment frauds as organised crime are also discussed. An examination of the response of law enforcement agencies—particularly the Fraud and Cyber Crime Group (FCCG) of the Queensland Police Service (QPS)—is detailed later in the chapter. That was an area raising significant controversy during the course of the Inquiry, resulting in interviews with a number of police officers and civilians, and five days of hearings. The hearings were held in camera due to the potentially sensitive nature of the evidence.

As a result of the information and evidence received, the Commission has made a finding that the QPS has failed to adequately respond to complaints from persons claiming to have been defrauded by people operating boiler-rooms.

Before turning to cold-call investment frauds in some detail, it is necessary to first make brief mention of real estate fraud, and Ponzi schemes generally.

### 5.2.1 Real estate fraud

Real estate fraud does not appear to be a current organised crime problem in Queensland, notwithstanding that it is well-known that investment in real estate is an established money-laundering method. Australia has been described by some as a ‘softer target’ for ‘dirty money’ investments in real estate, with a particular concern in respect of the continued exclusion of real estate agents from the reporting regime established by the Anti-Money Laundering/Counter Terrorist Financing Act 2006 (Cth) (the AML/CTF Act). Real estate as a money-laundering ‘channel’, and the AML/CTF regime, are discussed in more detail in the following chapter.

In respect of specific instances of real estate fraud, the Commission learned of two examples in Western Australia, and one in the Australian Capital Territory, where criminals based overseas were able to effect the transfer of property without the knowledge of the title holders. Those examples have prompted the Commission to make recommendations for strengthened identification verification requirements for real estate transactions in the section titled Related activities, below.

A number of historical allegations of real estate fraud in Queensland were also brought to the attention of the Commission.

In one case, the allegations centred on the use of ‘put and call options’ in real estate transactions. That case was the subject of a police complaint in 2009 (and subsequent complaints about police inaction), and a concluded civil claim. The QPS conducted an investigation, and decided that no charge(s) should be laid. A subsequent assessment by the Case Assessment Committee, within the then-Fraud and Corporate Crime Group (now known as the Fraud and Cyber Crime Group, or FCCG) affirmed that decision.

Another case allegedly involved a loan, a bank guarantee and the involvement of underworld figures to defraud individuals, banks and the Australian Taxation Office (ATO). The conduct complained of occurred in 2006 and 2007, and is currently the subject of judicial proceedings.

The Commission has determined that because of the age of the complaints, and given that the latter is the subject of current judicial proceedings (and thus excluded from consideration by the Commission’s Terms of Reference), neither matter falls within the scope of the Inquiry and, therefore, has not been considered for the purpose of this report.
5.2.2 Ponzi schemes

‘Ponzi’—or pyramid investment—schemes involve the offer of high returns on investments in, for example, computer prediction software or sports arbitrage schemes. Typically, victims’ investments are either immediately fleeced, or partially paid back in the form of supposed ‘returns’ to give the veneer of success. Those returns are, in fact, the victims’ own money—or that of other duped investors—and are sometimes abnormally high in order to encourage further investment.7

In its initial submission in May 2015, the QPS told the Commission that it ‘has investigated some cases where networks have operated boiler-room/call centre structures or ‘Ponzi’ schemes in the Gold Coast and Brisbane area.’8 Two examples were given. One, involving a man named Lovell, is an example of a large-scale fraud that evolved from a legitimate investment scheme. The case is described by the QPS as ‘a good example of the challenges associated with responding to these types of fraudulent schemes’, stating further that:

It is often very hard to distinguish between schemes that are entirely fraudulent from the start versus those types of schemes that may have begun in good faith but fail due to poor business management of investment structures or are operated by under skilled individuals.

... Whilst the ‘Ponzi’ style scheme used in R v Lovell [2012] QCA 43 reflects the types of business structures used by organised crime groups to commit financial fraud, the arrangements do not reflect traditional definitions of organised crime where multiple offenders are involved. Whilst the structure was well organised and engaged 14 employees including traders and analysts, the fraudulent activity was carried out by a single individual.9

A summary of the case is set out below. It is noteworthy that Lovell had gone to considerable lengths—and spent considerable sums of his ‘investors’ money—in unsuccessful attempts to obtain a financial services license. Lovell knew that such a license was a necessary precondition to lawfully operate a licensed investment company and solicit investment from the public at large.10 Notwithstanding his lack of success, Lovell was able to continue to operate without the license.

Case study

R v James Kentwell Lovell11

James Lovell pleaded guilty in the District Court at Brisbane to three counts of fraud and four related offences in relation to the operation of a ‘Ponzi’ scheme. Lovell was effectively sentenced to 13 years imprisonment. On appeal to the Court of Appeal, the sentence was reduced to 11 years imprisonment with parole eligibility after serving four years.

Lovell’s fraudulent offending was described as ‘gargantuan’. It spanned a period of six years, during which time he defrauded his investors of a total of almost $11.5 million. The Ponzi scheme involved the operation of three companies: Mirtna Holdings Pty Ltd (Mirtna Holdings), Life Super Pty Ltd (Super) and Mirtna Capital Pty Ltd (Mirtna Capital).

Lovell’s scheme commenced with the incorporation of Mirtna Holdings, a company which traded in securities, shares, options and futures. The Court of Appeal found that there was no reason to conclude that Mirtna Holdings was incorporated for fraudulent purposes, rather, that Lovell had ‘initially hoped, perhaps without reasonable cause, to build a genuinely profitable business.’

Lovell made representations that he had skill and knowledge, in addition to a software program, and that he had traded successfully for many years.
He initially introduced his friends and acquaintances to the scheme. Lovell told these investors that their funds were pooled and invested by him through brokers in Australia and overseas. As Lovell provided investors each month with statements indicating that their investment was increasing in value, they in turn recommended the investment to other friends and acquaintances.

Lovell subsequently incorporated a second company, Super, so that investors could roll over their superannuation monies held in other funds. Brochures were produced, extolling the benefits of investing in these companies. The brochures contained graphs that illustrated the monthly returns on investments, which were said to average between six and eight per cent per month. At one stage, according to the brochure, the annual growth in investments was 88.84 per cent and the average annual return over a five-year period was said to be 111.43 per cent. These statements were, of course, untrue.

Investors who wished to withdraw funds had to give notice, and these funds were, in fact, paid from funds subsequently invested.

Lovell then incorporated the third company, Capital, through which he intended to operate a licensed investment business. In order to do this, he had to obtain a Financial Services Licence. Lovell incurred considerable debts in his attempt to qualify for the license, and he repaid those debts from the monies paid to him from investors.

Chesterman JA, who disagreed that the original sentence was manifestly excessive, noted that:

[L]ess than a fifth of what he was paid was invested and he managed to lose two thirds of that. He never traded successfully, never made a profit, invested a fraction of the monies given to him for investment and he lied elaborately, persistently and flagrantly about the fate of the monies entrusted to him.

The Commission’s attention was also drawn to a case involving a man named Henderson. *R v Henderson* [2014] QCA 12 is a more recent case, and an example of a particular type of ‘Ponzi’ scheme that employs the use of aggressive telemarketing tactics and slick marketing campaigns—including sophisticated web sites, fake investment reviews and glossy brochures. Those types of cold-call investment frauds became the focus for the Commission, which found them to be a current, serious organised crime problem in Queensland.

5.2.3 Cold-call investment frauds (boiler-room frauds)

As indicated, these types of frauds are usually initiated by ‘cold-calling’ potential victims. The calls are made by persons employed in call centres. The call centres have been colloquially referred to in the media and by law enforcement agencies as ‘boiler-rooms’, due to the high pressure sales tactics used to persuade investors with promises of high returns.

Recent intelligence suggests that boiler-room operations on the Gold Coast are being run by syndicates involved in organised crime. They are complex and slick operations that use ‘phoenix’ tactics to avoid detection:

The southeast corner of Queensland seems to have developed a hub for boiler-room operations. They’re sophisticated in their product development and they’re highly flexible and mobile which means that the trail is always cold by the time law enforcement are alerted to the problem.\(^1\)

Detective Superintendent Brian Hay has been quoted in the media as saying that the Gold Coast has become a mecca for boiler-rooms. In an interview with the Commission he stood by that statement,\(^1\) but stopped short of referring to the current problem as an ‘epidemic’, preferring to refer to it as a ‘significant problem’.\(^1\)

Ken Gamble, a private investigator who has taken particular interest in the problem, told the Commission that, in his view, the QPS is responsible for the proliferation of boiler-room type fraudulent activity on the Gold Coast, because for the last five years, it has failed to investigate complaints—despite the ever-increasing
number of those complaints. That issue is discussed further in the section on responses to organised financial crime.

Boiler-room frauds have a number of typical features. Those known characteristics have allowed the QPS to develop a ‘life cycle’ of a boiler-room, described below. Understanding the life cycle of a boiler-room is critical, because the syndicates that operate them use various tactics to give their schemes a veneer of legitimacy, and often engage in fraudulent ‘phoenix’ activity to morph one scam into another in order to avoid detection.

The life cycle of a boiler-room

Boiler-rooms have a short life cycle; most are in existence for between six to twelve months. That is not to say that the criminals behind the boiler-rooms cease carrying on fraudulent activity. A syndicate might operate for many years, with a number of boiler-rooms created and later dismantled to avoid detection, before ‘phoenixing’ into a reincarnation of the fraud.

The Commission found that boiler-rooms have been active on the Gold Coast for many years with many of the same ‘players’. Detective Senior Sergeant Tiernan informed the Commission that:

> They’d been going since – they’d been continually looked at since about 2007 to 2009, and a lot of the same people were involved, ie [sic], the same offenders, the same networks, syndicates.

According to a QPS intelligence assessment from January 2015, a typical ‘boiler-room’ has a number of common features:

- A business (company) is established by the principal operator and, in the majority of cases, dummy directors are registered with the Australian Securities and Investment Commission. The company usually has a professional looking website.
- A call centre is established and telemarketers recruited, mostly locally. An office is fully equipped with telecommunication equipment and the telemarketers are provided with leads and the script. The telemarketers are usually not aware of the ‘true’ purpose of the business although some of them may have some suspicions about the business’s legitimacy.
- The callers are very persistent, often harassing victims by calling them several times a day.
- There is an implied ‘hierarchy’ of cold callers, whereby the victims are often referred to a manager or more senior investment adviser. This creates another layer of trust and offers a sense of validation to the victim.
- The cold calling company names are often very similar to a legitimate company, in an effort to piggyback on their good reputation and success.
- Victims are referred to websites which appear to be impressive and legitimate. The victims are often offered a demonstration of the software, which shows how the software works and its effectiveness.
- The fraudulent websites have information attesting to the success of the initial investment and, based on this information, the victim often invests more funds.
- Professional facilitators are used to provide investment advice used in cold calling scripts, to provide fraudulent identification to open bank accounts, to create companies, and to create internet accounts and professional websites.

‘Boiler-room’ operators often engage in the following types of fraudulent conduct to manipulate potential investors:

- They provide verbal promises to victims about the nature of the investment and have them sign a contract that states something entirely different. The victims either do not read the contract or they do not question it.
• They are evasive in their explanation of the investment and use language such as ‘a platform’ when describing the type of investment.
• They make outlandish claims as to the returns expected from the investment.
• They develop professional looking websites and glossy brochures.
• They provide a ‘live’ demonstration of their software, with the results being manipulated to make it appear as though they are making gains.
• After the initial ‘successful’ period, the victims are encouraged to sign up for a ‘more advanced platform’ with the promise of even higher returns, and are often asked to refer the company’s services to their family and friends.

Many of those typical features of boiler-room fraud were present in the case of *R v Henderson* [2014] QCA 12, summarised in the case study below:

**Case study**

*R v Mark David Jon Henderson*[^20]

Henderson stood trial in the District Court at Brisbane, charged with one count of fraud. He was found guilty by a jury after a 13-day trial, and was sentenced to nine years imprisonment with a parole eligibility date after serving four years.

Henderson, through his company, Sports International Investment Corporation Ltd (Sports International), received 173 payments from 59 complainants, defrauding them of a total of $1,832,991.00.

Each of the complainants were enticed to invest in the scheme after receiving repeated telephone calls from a person who identified himself as Peter Smith or Peter Armitage. Smith told prospective investors about an investment scheme associated with sports betting or sporting events, which was guaranteed to generate high returns. Smith has been identified as a co-accused of Henderson. Peter Armitage was a non-existent person and a pseudonym used by persons who called the complainants. Complainants were also induced by written materials containing what purported to be past records of significant gains made from sports investments. In some instances, the materials contained a guarantee of the principal sum invested, with representations that the scheme had been underwritten by Lloyds of London.

Complainants were required to enter into a contract, pursuant to which they would pay a substantial amount to purchase the service of Sports International and for trading purposes. Under the contract, the complainant was prevented from withdrawing any funds from the Sports International investment account for the first 12 months.

Complainants were provided with a username and password to log on to an associated entity referred to as ‘the Armitage’, where they could monitor the value of their investment. During the 12 months when customers understood they could not withdraw funds, they were nonetheless inspired by what appeared to be an astronomical growth in the value of their initial investment, and some made additional investments.

An analysis of the bank account into which the complainants paid their money revealed that the amounts paid by complainants were not invested in the interests or ventures they were intended for.

A virtual office facility was used to give complainants the impression that Sports International was located at Level 20, Tower 2/201 Sussex Street, Sydney, when in fact the scheme was being operated from premises at Bundall on the Gold Coast.
The complainants gradually discovered that they could no longer establish contact with anyone associated with Sports International or the Armitage. Every one of the 59 complainants lost the whole of their investment.

The telemarketers employed by Sports International were given databases also known as ‘lead sheets’ from which they would call potential investors.

The learned sentencing judge described the offending conduct as an ‘exceptionally serious example of fraud involving a sophisticated scheme.’ His Honour regarded the scheme as being ‘predatory in nature’ and reflected on the ‘significant adverse financial impact upon the complainants.’

His Honour was not able to conclude however, that Henderson was the central architect of the scheme, but was satisfied that he was involved from the early stages.

The Court of Appeal dismissed the appeal against conviction and sentence.

Fraudulent phoenix activity

As already mentioned, one of the ways in which operators of ‘boiler-rooms’ seek to avoid detection and conceal assets is by engaging in ‘phoenix’ activity. That involves using ‘puppet’ or ‘dummy’ directors to disguise the true identity of the principal operators of a business. Existing companies with a clean corporate record are chosen, so that would-be investors are satisfied with due diligence inquiries made with the Australian Securities and Investments Commission (ASIC).

It was suggested by Detective Superintendent Hay that the ease with which a person can register a company with ASIC has contributed to the difficulty facing would-be victims:

…It’s easier to … become a director of a company and register it than to get a video card, because at least the video company normally asks you to provide identities [sic] Whereas you can actually acquire – become a company director online and go through the process with no validation. And everyone makes the assumption …that if they’re registered with ASIC, that means they’re legitimate because they’ve been checked out, which is clearly not the case. 21

Once the fraudulent nature of the scheme is discovered and investors begin making demands for the return of their money—or complaints are made to law enforcement or regulatory agencies—the company is placed into liquidation, allowing the fraudsters to avoid paying back money to duped investors, or any debts owed to creditors. 22

The major assets of the company are typically protected in associated entities, allowing the business operators to continue uninterrupted by incorporating a new company and transferring employees from the company in liquidation to the new company.

An analysis conducted by the ACC has found that entities may be repeatedly incorporated and liquidated, as often as is required to keep the fraudulent scheme in operation. This fraudulent phoenix activity allows operators to maintain relative anonymity, in the hope of avoiding liability for investments that have been misappropriated or otherwise lost, and in order to continue to operate the boiler-room fraud under a fresh cloak. 23

A Phoenix Taskforce has been established by the Inter-Agency Phoenix Forum in an effort to better detect and deter fraudulent phoenix conduct. 24 The taskforce comes within the ambit of the Commonwealth Government Department of Education, and the focus seems to be on ensuring that employee entitlement and taxation obligations are met by those who seek to use phoenix activity to avoid them.

The following case study is of a recent, successful investigation and prosecution of a cold-call investment fraud that involved multiple companies and the use of a ‘dummy director’. 
Case study

R v Carlisle and Crouch\(^{25}\)

Carlisle and Crouch were sentenced in the District Court at Southport on 30 July 2015, and were each sentenced to a term of 10 years imprisonment for their part in a multi-million dollar fraud.

The men were arrested following a joint investigation, code-named Operation Juliet Dynamite, involving the QPS, the ACC and ASIC. The investigation was commenced after the QPS received complaints from more than 400 individuals, who had invested more than $5.6 million with Gold Coast companies offering the opportunity to invest through index trading. During the investigation, Crouch, Carlisle and their associates were placed under physical surveillance and their telephone conversations were intercepted.

To facilitate their fraud, Crouch, Carlisle and their associates set up five companies, which operated between December 2010 and December 2011. Each of these companies leased office space and employed a number of telemarketers who initiated contact with potential victims.

Each of the victims was cold-called and offered non-existent investment opportunities. Once interest was shown, the victims received a glossy brochure and were encouraged to refer to a website for additional information. There was a follow-up call about one week later, followed by an email attaching documents titled ‘License Agreement’, ‘Guarantee,’ and ‘Client Application Form.’ Each of the victims returned the forms and subsequently transferred money to a nominated bank account. Once funds were deposited to the nominated bank accounts, they were promptly withdrawn.

Some of the victims were granted access to the company website so that they could monitor their investments. After a short period, however, access to the website was denied and attempts to make contact with the company by phone or email proved fruitless.

Crouch and Carlisle managed the boiler-room operation at each location. Despite this, their names do not appear on any of the company documents, leases, bank accounts or other business records. Even their mobile telephones were subscribed under false names.

Associates of Crouch and Carlisle withdrew large sums of cash over the counter at bank branches on the Gold Coast or from ATMs and delivered the money to Crouch and Carlisle. Some of the money was used to meet operating costs, such as the payment of rent on leased premises and the payment of retainers for the telemarketers. There is no evidence of what happened to the money after it was delivered to Crouch and Carlisle, although there are indications that there were other persons involved in the boiler-room operation who were higher up the pyramid than Crouch and Carlisle.

During the investigation, police seized a total of $179,000.00. Just prior to the arrest of Crouch and Carlisle, the funds remaining in the bank accounts were frozen. Only $585,987.60 remained.\(^{26}\)

One of the above-referenced associates who assisted Crouch and Carlisle was a person named Lewis. Lewis appeared in the District Court at Southport for sentence on 23 January 2015. Lewis pleaded guilty to one charge of money laundering. He was sentenced to a term of 12 months imprisonment, wholly suspended for a period of 18 months.

Lewis was 54 years of age during the offending period. He had been unemployed for an extended period, and had alcohol and drug addiction problems. Lewis agreed to be nominated as the sole director of one of the companies used by Crouch and Carlisle as a vehicle of their fraudulent operations. Lewis subsequently set up an account at the National Australia Bank, into which 33 victims deposited $440,515 over a period of about six weeks. Lewis withdrew a total of $400,369.91 from that account over the same period of time. To Lewis’s credit, when he was approached by police, he agreed to be interviewed by them and, in due course, made admissions relating to the role he played in the enterprise. He admitted to police that he took part in the scheme to make ‘a few bucks.’\(^7\)
In sentencing Lewis, her Honour, Judge McGinness, accepted that his actions:

...amounted to obtaining money whilst having no real concept of the serious nature of the criminal scheme perpetrated by the others as a whole. However, your actions, as I’ve indicated, do amount at the very least to reckless behaviour and a form of wilful blindness to the activities that generated the money that you deposited and withdrew...there was an aspect of greed in your behaviour to feed your alcohol problem and to obtain money easily for little effort.....although you were a minor participant, your involvement was necessary to allow the criminal enterprise to operate and flourish.27

Types of cold-call investment frauds

The types of investment opportunities offered under these fraudulent schemes vary. The Commission learned of examples involving the manipulation of the stock market,28 computer prediction software,29 and sports arbitrage. Recovery schemes are also used in a particularly cruel way, to entice duped investors to put money into a ‘fighting fund’ with other victims, with the promise of trying to recover the original investment. A brief summary of the types of scams offered follows.

Share index trading

In this type of fraud, investors are persuaded to invest money with a company that markets itself as being in the business of index trading. The company represents that it has some special skill and knowledge in this area. Investors transfer money into a designated bank account, believing that it will be applied to index trading by experts employed by the company. Investors are each given a personal login so that they can monitor the progress or growth of their investment. In actual fact, the money invested is not re-invested in index trading at all. The operators of the scam gradually withdraw the money from the account in cash. They do this by presenting cash cheques over the counter or by withdrawing the cash from an ATM. Sometimes they use ‘mules’ to withdraw the money for them.

Stock market manipulation

Stock market manipulation scams are also referred to as ‘pump and dump schemes’. They typically involve the promotion of worthless stocks to increase the share price, for instance, by sending out false tips about a company having great prospects. As more people invest, the share price increases. The scammers then sell or ‘dump’ their shares at the peak of the price rise, causing the value of the shares to fall, leaving investors with shares that are either worthless or valued at a fraction of the purchase price.30

Computer prediction software

Some investment frauds involve betting and the sale of computer prediction software. Investors are attracted by promises that the software will accurately predict the outcome of horse races, other sporting events or stock market movements. Scammers make their money by convincing investors to pay membership fees and to purchase calculators, newsletter subscriptions and computer software programs.31

Sports arbitrage

Some of these scams involve investment in a sports arbitrage system, where the scammers claim that they have people trading on international sports markets who ascertain the best prices being offered on bets. Investors place money into a syndicate, betting or trading account. The operators of the scam represent that they place bets on behalf of investors on all participants in a contest, thereby guaranteeing a win.32

The Commission received information that this trading on international sports markets is commonly referred to as a ‘trading pod’.33 Investors initially purchase software that inevitably lures them into a ‘trading platform’. Investors are then given exclusive access to the trading pod, from which previous investors were allegedly making millions of dollars in profits. In the short term, the balance of these trading accounts—which are accessible online—appear to be ever-increasing, giving investors the impression that their investment has
been profitable, as was promised. In actual fact, behind the scenes, the scammers manipulate the online trading accounts to show profits that cannot possibly exist, because the money invested by victims in the trading accounts is not used to place bets, having been stolen by the scammers. The Commission received information that some of the major networks involved in ‘boiler-room’ fraud on the Gold Coast have successfully transferred millions of dollars overseas.34

**Recovery scams**35

Some victims of boiler room frauds are re-victimised in recovery scams. These are particularly cruel, in that victims are again ‘cold-called’ by a person purporting to represent a group of people who have fallen victim to the same scam. In this type of scam, the victim is then encouraged to contribute money to a ‘fighting fund’, which they are told will be used to recoup their money.

Often the operators of the ‘recovery scams’ are connected to the operators of the ‘boiler-room’ scams.

### 5.2.4 Organised nature of the crime

Cold-call investment frauds are recognised as a serious, organised crime issue. According to the ACC:

> …these sophisticated operators have been identified exploiting technology to develop what appear to be safe websites and environments and develop false websites providing potential victims with a sense that an investment opportunity is legitimate. Such practices suggest a high level of organisation.36

Boiler-room frauds cannot be described as an opportunistic crime. To the contrary, many such frauds have been found to be calculated, sophisticated and highly organised.37 Leaving aside the cost to individual victims, it is increasingly concerning that organised crime groups use the income they derive from these frauds to fund other criminal activities such as importing drugs, trafficking in firearms and, potentially, to fund terrorist activity. It is believed that some of Australia’s most notorious criminal identities have ultimate beneficial ownership of some of the companies operating boiler-rooms on the Gold Coast.38

The high level of organisation and sophistication of these operations becomes apparent in the methods adopted in an attempt to disguise not only the beneficial owner/s of the enterprise, but also the place of business and even the true identities of the telemarketers employed to promote the scam.39

Boiler-room operators use the services of professionals such as lawyers, company formation agents, and accountants to design complex corporate structures with the dual purpose of disguising the ultimate beneficial ownership of the enterprise and facilitating the laundering of the money invested by unsuspecting victims.

Companies involved in boiler-room operations have been found to have phantom or dummy directors. These are often people who have a limited or no criminal history. This ensures that if a potential investor or regulatory or law enforcement agency makes inquiries about these ‘cleanskins’, no suspicions will be aroused.

Solicitors are used to draft the contracts that are presented to investors, and IT specialists are employed to design and produce professional-looking websites. While an analysis undertaken by the ACC has found that some of these professionals knowingly provide their services to facilitate criminal activity,40 the Commission has not found evidence that this is a widespread practice, and it appears that most of these professionals provide their services unwittingly.

Staff employed by boiler-room operators are provided with aliases or false identities. They are provided with a list containing the names and other personal information of people they will ultimately call (referred to as ‘lead’ lists), and are provided with a script that is usually prepared by a professional such as a financial advisor. When call centre staff telephone potential investors and rely on the script, they give the impression of having some level of knowledge or expertise in the area they are dealing with. This in turn helps to create an air of legitimacy, and if potential investors have any reservations about the investment, such reservations are easily dispelled.
Further, boiler-room operators often use virtual offices to disguise the true location of the boiler-room and to add gravitas to the operation (by having a Sydney City address, for example). This practise might point law enforcement agencies in the wrong direction, initially, and cause confusion for victims regarding where their complaint ought properly be made.

5.2.5 Prevalence

In 2011, Taskforce Galilee\footnote{41} described ‘boiler-room’ fraud as ‘Serious and Organised Investment Fraud’, which it defined as follows:

\begin{quote}
Any unsolicited contact, by telephone or internet, of persons in Australia (potential investors) by persons (callers) usually located overseas, where such callers engage in conduct that is fraudulent, false, misleading or deceptive with the purpose of inducing potential investors to buy, sell, or retain securities or other investments and where such callers do not have the license or authority to engage in a securities business, or investment advice business in Australia...\footnote{42}
\end{quote}

The Commission has found that, although traditionally committed by criminal syndicates operating from overseas, ‘boiler-room’ frauds are increasingly being perpetrated by criminals who have set up their operations on the Gold Coast. According to QPS intelligence as at January 2015:

\begin{itemize}
\item A growing number of criminal syndicates involved in boiler-room fraud have been operating from the Gold Coast.
\item The growing ‘success’ of boiler-room fraud can be attributed to the use of professional facilitators, especially IT and communication experts.
\item It is estimated that the potential loss to ‘boiler-room’ fraud in Australia amounts to tens (possibly even hundreds) of millions of dollars each year.
\item Large amounts of money have been sent overseas using sophisticated money-laundering schemes.
\item There are at least six major organised crime syndicates operating boiler-rooms on the Gold Coast.\footnote{43}
\end{itemize}

Although there has been a steady increase in the last few years in the number of complaints made about boiler-room fraud, ‘this is still not reflective of the true extent of the problem.’\footnote{44} Like other types of financial crime, boiler-room frauds are notoriously under-reported. The QPS intelligence assessment from January 2015, provides some possible explanations:

\begin{itemize}
\item Some victims consider this as a bad investment decision, thus accepting their loss.
\item There is a general perception that police do not take their complaints seriously.
\item Some victims are embarrassed by what happened and are keeping it to themselves.
\item Some victims are hoping to recoup their money by falling for another similar scheme and become scammed multiple times.
\item The time delay between the initial investment and the realisation that they have been scammed can be significant, and their subsequent complaints are often months and sometimes year olds.
\item A number of complaints have been made to the Australian Securities and Investment Commission and the Office of Fair Trading, but not the QPS.\footnote{45}
\end{itemize}

Information provided by the QPS, again based on intelligence current as at January 2015, suggests that the total amount of reported losses to boiler-room fraud in Queensland in 2014 was $7.5 million,\footnote{46} and that at any given time, between 20 and 30 boiler-rooms are operating on the Gold Coast.
5.2.6 Impact on the victims

A recent report by the Australian Consumer and Competition Commission (ACCC) reveals that investment fraud and computer prediction software scams are among the most damaging scams in Queensland in monetary terms. They rank at number two (investment schemes) and three (computer prediction software and sports investment schemes) on a list prepared by the ACCC, with the number one scam position occupied by dating and romance scams.

A table setting out the monetary loss to Queenslanders from various types of fraud—including these—is reproduced in the section on financial data theft, below.

According to the ACC, the consensus among Australian law enforcement and regulatory agencies is that the most-likely persons to fall victim to boiler-room fraud in Australia are:

- middle-aged to older persons (often over 35 years, but usually over 50 years old)
- male
- small business owners
- self-funded retirees
- individuals who have previously made investments in other companies and were considered ‘financially literate’
- individuals who are on shareholder registers
- socially isolated individuals – geographically or otherwise

It would be a mistake to assume that the persons who fall victim to these frauds are uneducated. To the contrary—many of the victims have a high financial awareness, are well-educated and have invested previously. People are rendered vulnerable by life events. Anyone at any time can become a victim to these frauds. The many impacts on victims include the following:

- financial devastation for individuals and their families—including, in some cases, loss of all of their retirement funds
- ongoing debt - victims who borrowed money to invest still have to repay the borrowed sum and interest—those who default on their repayments may have remaining assets, such as the family home, repossessed, or they may face bankruptcy
- loss of credit rating - making it difficult for victims to rebuild their financial position
- loss of life savings compounded by factors such as age or illness – victims are sometimes not able to work and are left facing a poor future
- stress, anxiety and depression – in extreme cases leading to suicide
- isolation or estrangement of victims from family and friends
- feelings of guilt, shame and embarrassment

The cost of financial crimes to the individual victim can be significant, and extends beyond dollar costs. Moreover, the social, economic, physical and psychological harm caused by these crimes impact on the community and economy as a whole.

(Endnotes)


10. R v Lovell [2012] QCA 43 at [34].


17. Transcript of hearing, Stephen Tiernan, 20 July 2015, lines 31–33, p. 82.


26. Response to issued notice, Queensland Director of Public Prosecutions, 21 August 2015.

27. R v Lewis (Unreported, District Court of Queensland, McGinness DCJ, 23 January 2015).


33. Submission of Ken Gamble, 24 June 2015, p.16.

34. Response to issued notice, Queensland Police Service. State Intelligence -
Intelligence Assessment: ‘Boiler room’ Fraud on the Gold Coast, 5 January 2015, p. 4.


41 Taskforce Galilee comprised of law enforcement, regulatory and service delivery agencies across federal, state and territory government. Taskforce members included all Australian Crime Commission Board agencies as well as the Australian Competition and Consumer Commission, the Department of Broadband, Communications and the Digital Economy, the Department of Immigration and Citizenship, the Department of Human Services and the Australian Transaction Reports and Analysis Centre.


44 Queensland Police Service. State Intelligence - Intelligence Assessment: ‘Boiler room’ Fraud on the Gold Coast, 5 January 2015, p. 3.


5.3 Financial data theft

5.3.1 Overview

For organised crime groups, the theft of card data is the primary means of financial data theft. Common methods used to steal financial data include ‘card-not-present’ fraud schemes, ‘skimming’, ‘phishing’, the use of ‘malware’ and ‘ransomware’, and hacking. The nature of those crimes, their prevalence, and impacts to the community are addressed below.

Although card data theft is the most prevalent means of financial data theft, other methods include harvesting financial or identity information stolen from documents—including from superannuation account information and utility bills. Once authentic data is obtained from those documents, offenders are in a position to create false bank accounts and derive cash in other ways.

The Commission identified other prevalent financial crimes that are perpetrated by organised crime syndicates but which do not fall easily into the categories of investment and financial market fraud and financial data theft. Those crimes include advance-fee frauds, email scams and romance scams, whereby victims are duped through fraudulent means, resulting in significant financial loss. Those crime types are addressed in the section on scams below.

Identity theft is commonly referred to as an enabler of organised crime (including in the Terms of Reference), and for that reason it is referred to in detail in the section titled Related activities. However, identity theft is also a crime type itself.

The Australian Crime Commission (ACC) describes identity theft as an under-reported and prevalent crime type, describing activities in which a perpetrator steals a person’s identity or uses fabricated, manipulated, stolen or otherwise assumed identity to facilitate the commission of a crime.1 It is commonly inextricably linked with financial data theft.

Cyber and technology-enabled crime is also often intimately linked to financial crime. Although traditional and novel methods of obtaining a financial advantage continue, the age of the Internet has resulted in increasing cybercrime, such as phishing, hacking, and email scams to effect a fraud on victims or to steal information.

Data kept by the Australian Cybercrime Online Reporting Network (ACORN) supports the suggestion that financial crime is increasing, particularly in the cybercrime environment. ACORN commenced as a national policing initiative in late 2014, with collaboration between state police forces, the ACC and various other agencies. It allows direct reporting of cybercrime via an online portal and is a key initiative of the National Plan to Combat Cybercrime. ACORN statistics reveal that of offences reported in May 2015, 59 per cent were reported as online scams or fraud.

Anecdotally, the number of Queensland offences reported to ACORN are far greater than expected. Detective Senior Sergeant Stephen Tiernan told the Commission that when ACORN was initially proposed, the Queensland Police Service (QPS) anticipated reports of seven to eight cybercrimes a week. In fact, on average, there have been 33 reports a day.2

Reporting statistics gathered between January and March 2015 and published in an ACORN Snapshot (extract below) placed Queensland as having the second-highest number of complaints of all states and territories.3 The demographics indicate that people aged between 20 to 40 years are either most susceptible or most likely to report cybercrimes, with 40-to-60-year-olds not far behind.

The top three cybercrimes reported are scams or fraud (49 per cent), purchase or sale (24 per cent) and cyber bullying (7 per cent), while the top three targets of cybercriminals are email, social networking and website advertising.
Organised crime and cybercrime are increasingly overlapping. As suggested by the statistics above, cyber and technology-enabled crime clearly facilitates the commission of financial crimes. Similarly, identity crime is intimately linked to financial data theft and scams. The theft of account data often involves the compromise of some identity information, and the duping of victims involves some assumption of other identity information to perpetuate the ruse. Consequently, it is almost impossible to consider financial data theft without also considering identity crime (referred to in detail in the section titled Related activities). Money laundering (addressed in the following chapter) is another enabler of financial crime (along with other types of organised crime), allowing criminal networks to ‘clean’ the profits and cover the trail.

Those enablers of financial crime make detection and investigation difficult, requiring significant cooperation across state and national borders. The response to financial crime can also be compromised by a perception that it is not ‘serious’ crime when compared with offences against the person and drug offending, and because police officers are often daunted by the apparent or comparative complexities of fraud.

### 5.3.2 Card fraud, financial documents and identity theft

#### Traditional methods

Traditionally, financial data has been stolen opportunistically and in targeted attacks by stealing physical documents or items (such as a wallet or credit card), by intercepting mail, and by ‘dumpster diving’ for specific documents. The ACC reports that theft of cards from the mail has increased, particularly since 2013. That might be due to less-sophisticated criminal entities reverting to the theft of genuine cards to overcome the challenge posed by chip technology and PIN security. Contactless payment (for example, by using Paywave) also allows for small-scale card fraud by those in possession of genuine cards.

With access to financial documents, in combination with either forged or stolen identity documents, offenders are able to create false bank accounts and fraudulently obtain funds from financial institutions.

#### Card-not-present fraud

Card-not-present fraud (sometimes referred to as ‘CNP fraud’) involves the theft of information attached to a credit or debit card (often including the Card Code Verification (CCV) number) while the card-holder retains possession of the card. The data can then be used without the knowledge of the card-holder, usually to make purchases online. Compromised transactions often occur outside Australia, making it easier for cardholders to identify the fraud and seek reimbursement from their financial institutions.
Given that financial institutions generally wear the cost of card-not-present fraud, and do not necessarily forward complaints to law enforcement, it is difficult to assess how much of this type of fraud is perpetrated by organised crime. It is clear, however, that significant financial loss is caused. That consequence flows to the community by way of increased costs associated with holding bank accounts.

According to the Australian Payments Clearing Association, card fraud rates have increased over the past year from 46.6 cents to 58.8 cents for every $1,000 spent. The majority of that increase is attributable to the rise in card-not-present fraud.\(^3\)

Card-not-present fraud rose to $299.5 million in 2014, from $210.4 million in 2013, with two-thirds ($200.6 million) occurring overseas (an increase from $124.5 million in 2013).\(^6\) Given that context, much of it is likely to be committed by organised criminal networks. The Australian Payments Clearing Association media notes that along with continued strong online spending by Australians, the following factors also provide context to the increase:

- As industry measures to reduce payments fraud in one area take effect (for example, through the use of chip technology), criminals switch to other areas where frauds are easier to perpetrate.
- The online environment is being targeted more widely by criminals generally, with card-not-present fraud just one manifestation of the growing threat from cybercriminals experienced by governments, businesses and individuals worldwide.\(^9\)

The movement of fraud from the face-to-face environment to the cyber environment is demonstrated by the changing prevalence of card-not-present fraud compared with counterfeit/card-skimming fraud. This ‘migration of fraud types’ is demonstrated below in graphic representations taken from the Australian Payments Clearing Association’s 2015 Australian Payments Fraud: Details and Data Report.\(^10\)

![Graph showing the change in total Australian card fraud type from 2009 to 2014.](chart)

The fraudulent acquisition of card data and the use of that data is a ‘market’ dominated by overseas-based groups.\(^11\) In fact, two-thirds ($200.6 million) of card-not-present fraud occurred overseas in 2014 (up from $124.5 million in 2013).\(^12\)

As at March 2015, a QPS intelligence assessment identified offenders from Cambodia, Ghana, Indonesia and Malaysia as committing the majority of card-not-present frauds on Australian online retailers. Offenders identified in Cambodia are mostly of Nigerian heritage.\(^13\) According to the QPS, the cost of card-not-present fraud to Australian retailers was $124 million in the 2013–2014 financial year. That figure does not seem to be restricted to online retailers and does not include attempted frauds.\(^14\)

Technology and the cyber environment facilitates the on-sale of stolen financial and identity data, particularly through use of Tor and the Darknet with the attendant benefits of anonymity. For example, the ACC located one Darknet site selling cards for 8 cents, card code verifications (CCVs) for $8, and other card details—including billing addresses—for $80.\(^15\)

Insofar as other identification information is concerned, Mr David Lacey, Managing Director of iDcare (a non-government identity theft support service), told the Commission that as part of current research in the area of
identity crime and the Darknet/Deep Web, IDcare has learned that Queensland Transport Drivers Licenses are available for purchase.\textsuperscript{16}

The QPS intelligence assessment also suggests that card details are often sourced on the Darknet. Various methods are used to obtain a benefit from the card data, but often ‘money mules’ are hired to send fraudulently obtained cash or property to perpetrators.\textsuperscript{17}

Some ‘money mules’ are foreigners, offered financial or other incentives such as student visas. Others are recruited from within Australia, often by grooming through a romantic relationship. Several such ‘mules’ have been interviewed by police, with many unaware of the illegality of their conduct.\textsuperscript{18} The QPS intelligence assessment of March 2015 recommends that once those ‘money mules’ have been identified, a letter should be sent advising the ‘mule’ their activities are illegal. It is further recommended that details of such letters be recorded in the QPS Management Exchange (QPRIME) system to assist investigators in proving knowledge should the ‘mules’ continue their conduct.\textsuperscript{19} It is not known whether this has progressed from recommendation to action.

Organised crime groups are also known to recruit ‘financially vulnerable individuals to participate in shopping holidays to Australia.’\textsuperscript{20} Those recruits come to Australia, make purchases on counterfeit cards stored with the stolen data, and then send the fraudulently obtained property back to those organising the scheme.

The reporting of online frauds by retailers has been known to assist law enforcement agencies to identify ‘mules’ and the ultimate origins of such frauds. However, where complaints are made in isolation, it is difficult to identify links, and organised groups of offenders.\textsuperscript{21}

Centralisation of cybercrime complaints (including online fraud) to ACORN (Australian Cybercrime Online Reporting Network) may assist law enforcement agencies to identify modus operandi of offender networks. Anecdotal information provided to the Commission suggests that this has occurred. Now that ACORN has been running for approximately nine months, research or assessment of its efficacy may be beneficial.

Financial institutions have also moved to better protect themselves—for example, by introducing two-stage or two-factor authentication. A mechanism for information-sharing between retailers may also help prevent card-not-present fraud, enabling retailers who have identified certain IP addresses or credit card data as likely to be fraudulent, to share that intelligence with other retailers.

Skimming and counterfeit cards:

‘Skimming’ is the theft of credit or debit card data, by attaching a ‘skimming device’ to Automatic Teller Machines (ATMs) or Electronic Funds Transfer at Point of Sale (EFTPOS) machines (the latter usually requiring some assistance from dishonest staff). Such devices capture and store card data. Once removed, data is loaded onto blank cards with magnetic stripes, such as gift cards. At ATMs, pin-hole cameras have been installed to capture the customer’s Personal Identification Number (PIN), or, in more rudimentary examples, a ‘shoulder-surfer’ might observe a the customer enter the PIN. Cash can then be withdrawn from legitimate bank accounts, using new cards, without the customer or financial institution becoming immediately aware.

Successful prosecutions of skimming offences and intelligence from law enforcement suggests overseas syndicates of offenders are key perpetrators. Offenders fly (or are flown) into Australia and work the east coast of Australia over a short period before departing again. The stolen cash is often laundered into overseas accounts, using remitters (persons/entities who transmit money) such as Western Union to transfer amounts of less than $10,000. The Anti-Money Laundering and Counter-Anti-terrorist Financing Act 2006 (Cth) (AML/CTF Act) requires reporting entities to report ‘threshold transactions’ (those involving the transfer of $10,000 or more) to the Australian Transaction Reports and Analysis Centre (AUSTRAC).\textsuperscript{22}

Remitters are required to report all suspicious money transfers (also referred to as ‘SMRs’) and International Funds Transfer Instructions (IFTIs) in addition to those transfers over the threshold amount. AUSTRAC analyses transactions and shares information with law enforcement agencies, in turn assisting in identifying potential skimming offences and advance-fee frauds (see below).
The Commission was alerted to an issue with online IFTIs where the remitter’s servers are based offshore. Those transfers are not currently captured by the AML/CTF regime. The AML/CTF Act is currently subject to review. The Commission supports any recommendation to amend the AML/CTF Act to ensure that any online IFTIs with an Australian connection are captured.

Several skimming matters have proceeded to sentence in Queensland, resulting from investigations conducted by the QPS. Although a range of charges were preferred in those matters, the Commission noted a trend to prefer Commonwealth money-laundering offences. It may be that fraudulent conduct defined in the Criminal Code (Qld) was not apt to capture the nature of the offending, particularly where the complainant financial institution was not in Australia. This potential gap is discussed in the following chapter. Alternatively, it may be that, where fraud with a circumstance of aggravation could be proved, the maximum penalty under the Queensland legislation is only 12 years. In contrast, in certain circumstances the Commonwealth money-laundering offence carries a maximum penalty of 20 years imprisonment. A wider range of maximum penalties apply to Commonwealth money-laundering offences (‘dealing in proceeds of crime’). Where there is intent and the money or property is worth $100,000 or more, the maximum penalty is 20 years imprisonment. Recklessly dealing in $100,000 or more warrants a maximum of 10 years imprisonment, and negligently dealing in $100,000 or more attracts a maximum of 4 years imprisonment.23

A number of Queensland residents have been prosecuted for their roles in laundering illegally obtained funds from skimming as ‘money mules’. Those offenders were said to be less sophisticated, who were often provided a pre-filled form containing the destination account details.24 The ‘mules’ would use their own identification and sign the form.

In the following case study, a Romanian national (Alexandru Stroia) was sentenced on two distinct sets of money-laundering offences, with others involved in both.

**Case study**

**R v Stroia and associated offenders**25

In 2011, Alexandru Stroia and Mircea Flutur were prosecuted for money-laundering offences related to the ‘skimming’ of debit/credit card data from devices they had installed on ATMs. The data was cloned to blank magnetic strip cards. PINs had been captured by cameras also attached to the ATMs. The offences were committed between January 2009 and July 2010.

Stroia and Flutur were both Romanian nationals, based in London with no ties to Queensland or Australia. Flutur told the court he had become involved in the offending after meeting some other Romanians in Sydney. He had over-stayed his visa and was likely to be deported, after serving the 14 month non-parole period of his four-year sentence (the relatively short non-parole period was because the court could not declare his pre-sentence custody). The money Stroia and Flutur obtained from the offending was transferred internationally to the United Kingdom and Romania. Only a very small amount was located in their possession when arrested. Stroia was sentenced to three years imprisonment with a non-parole period of 18 months.

Within a few months of release, Stroia commenced offending in a similar way. He withdrew cash using cloned magnetic strip cards and remitted funds to his criminal associates overseas, transferring (or arranging the transfer of) over $569,890 in 118 separate transactions. The cash was stolen in Australia, but originated from Dutch bank accounts. On arrest, police seized $66,900. Stroia was sentenced for those offences in February 2015.

Stroia recruited and paid two others within Queensland to assist in the international transfers of cash: Owen Tovt and Jnaashil Bali Gautam. Both were also convicted and sentenced on money-laundering offences.
The criminal network expanded when both Tovt and Gautum recruited family members and associates to conduct international transfers on their behalf. One of those (Raymond Jenkins) was prosecuted and sentenced in the District Court.26 Nineteen others were prosecuted and sentenced for money-laundering offences in the Magistrates Court.

As with card-not-present fraud, financial institutions mostly wear the financial loss from skimming offences. Consequently, they have a financial incentive to counteract skimming offences, and have done so by educating customers to cover their hand when entering PINs, and by disrupting skimming with the installation of anti-skimming devices. Newer ATMs are better equipped to protect against skimming devices by, for example, protecting the keypad with a small shield. Thus, older ATMs are more likely to be targeted by offenders.

The advent of chip technology is expected to produce a decrease in skimming offences, because the data is stored on a chip and not on the card’s magnetic strip. The chip corresponds with the ATM in a particular way, which is currently difficult to reproduce. Anecdotally, chip technology has already reduced the prevalence of skimming offences, although the absence of significant ‘skimming’ activity may also be a result of under-reporting by financial institutions.27 Having said that, the Australian Payments Clearing Association has reported to the Fraud in Banking Forum that there is no issue of under-reporting.28

In any event, despite the 25 per cent reduction over the six years from 2009 (attributed to chip technology), 2014 saw counterfeit/skimming fraud increase by 17 per cent from 2013. That increase is said to be largely due to skimming attacks on ATMs. A move away from magnetic strips is expected to have a significant impact on reducing this type of fraud over the next few years.29

Government and industry continue to work to reduce vulnerability in online fraud and cybercrime. The Australian Payments Clearing Association reports that the payments industry is adopting a new measure known as ‘Tokenisation’. Tokenisation will see the replacement of sensitive information (such as card numbers) with a non-sensitive replacement value, making it much more difficult for criminals to steal card details to use fraudulently.30

The challenge for law enforcement in the future will be keeping up with the new technologies and methodologies adopted by organised crime syndicates to counteract chip technology.

**Phishing, vishing, spear-phishing**

The theft of financial data can also involve a ruse or scam designed to persuade consumers to provide their bank account details to the offender. These may be more likely to be reported to police than card-not-present or skimming offences, because the consumer has been targeted online or in their home by telephone, and can point to a recognisable instance when their data was compromised.

Phishing refers to emails designed to deceive the consumer, by purporting to be from a bank, a government agency or a seemingly legitimate business. The emails often seek confidential information, which enables offender/s to access accounts, or could contain links to fake websites where the recipient is required to enter their confidential information, which is then stored by the offender/s. Such emails may also result in malware being downloaded to the recipient’s computer if the recipient responds. In that case, a consumer may not realise until much later that their account has been compromised.

Vishing is similar to phishing, but utilises telephone or voiceover messages to persuade victims to provide identity or account information, purportedly to avoid theft or misuse of that information. Common examples include callers purporting to be from computer companies (for example, Microsoft), telecommunication companies, or banks.

Spear-phishing refers to more targeted examples of phishing (or vishing). Rather than setting an all-purpose trap, specific victims are tracked, with emails purporting to come from institutions particular to the victim.
Phishing and spear-phishing are likely to be categorised as cybercrime. Consequently, victims who report such matters to local law enforcement agencies are likely to be referred to the ACORN online portal to report the crime.

In 2006, an offender was prosecuted in Queensland for laundering money, obtained by another person who had apparently been phishing for bank details. The offender established a number of accounts and another person deposited funds obtained by phishing into those various accounts. The offender’s subsequent conduct in withdrawing and passing on the funds resulted in the money-laundering charges.

Malware and ransomware

Malware attacks are inflicted on both businesses and individuals, and are considered to be a growing risk. Victims unintentionally download malware, which, once downloaded, enables offenders to steal online banking details or, alternatively, make business servers or networks unavailable, temporarily suspending the system (denial of service).

Ransomware enables an offender to lock the target’s access to their own network and extort a ransom, also compromising data held by the target. A media report from June 2015 describes how hackers obtained sensitive information from a network, and then demanded a ransom for the files. The business made the payments, in Bitcoin. However, the attackers responded by making further demands and the business complained to police. The attackers then escalated the attack by threatening an executive and his family. Ransomware has received a lot of attention in very recent times. The Australian Competition and Consumer Commission (ACCC) has reported a spike in complaints, and already this year it has received a number of complaints similar to that received for the whole of 2014.

Malware and ransomware is further discussed in the section titled Related activities, below.

Hacking, pharming and keylogging

In relation to financial data, hackers may gain access to databases of companies or other agencies with valuable financial data. Motivations for hackers vary—including, for example, moral causes and activism (or hacktivism as it is sometimes referred to). The risk related to financial crime is that hackers can obtain primary financial information (such as bank account details and passwords), as well as secondary information (such as identity data), which may allow them to commit other offences or on-sell the valuable data.

Pharming refers to the re-direction of traffic from a legitimate website to a bogus site which has the appearance of the authentic site. Once re-directed, consumers may be required to input personal and confidential information, which is captured by the offenders. This offending is concerning because it gives organised crime the ability to infiltrate legitimate organisations without their knowledge and obtain identity and other valuable information.

Keylogging involves the use of specific hardware to capture keystrokes of victims, thus enabling confidential information to be obtained. Because it requires attaching a device to a computer, it is more common in Internet cafes and other environments where multiple computers are accessible by the general public.

Compromise of identity information

As with financial crime, identity theft is under-reported to law enforcement. Research conducted in 2012 by the Australian Bureau of Statistics revealed that only 50 per cent of credit card fraud victims and 66 per cent of identity theft victims reported the occurrence to any formal body, such as police or a financial institution.

The QPS submission to the Commission, referring to its 2014 statistics report, states that identity fraud has increased by over 30 per cent over the previous 2013 period. The ACC Organised Crime Report 2015 refers to an Australian Institute of Criminology survey where 9.4 per cent of respondents reported having personal information stolen or misused in the past 12 months, with five per cent having suffered financial losses.
The Commission interviewed David Lacey, Managing Director of iDcare (a non-government identity theft support service). Mr Lacey advised the Commission that once identity information is obtained, compromise usually occurs within 72 hours. Given that victims may not realise that their identity information has been obtained, it is hard to prevent that compromise. iDcare assists victims in the process of restoring their identity. According to a new report in May 2015, the most common complaint was theft of drivers licenses. The theft of a key form of identification presents a much greater risk of future loss than that of credit/debit cards or data.

Case study

Identity theft reported to iDcare 1 July 2015

After a break-in on 29 June 2015, a couple contacted iDcare reporting that the following items were stolen:

1. Credit/debit card
2. Medicare details
3. Australian Tax Office Tax File Number(s)
4. Bank account details
5. Mobile phone information
6. Birth/death/marriage certificates
7. Superannuation information
8. Firearms licence
9. Login information and online passwords
10. Copies of share account establishment forms, including signatures and other personal identification information

At the time of contacting iDcare, bank account funds of $2,000 had already been misused, as had credit cards. The couple had started receiving bizarre phone calls from as far away as the Philippines. They remain concerned about the offender(s)’ ability to use their details and signatures to steal their investments, superannuation and savings.

Victims are able to obtain an 'Identity Certificate' from courts, post-conviction of an offender (section 408D Criminal Code (Qld)). Mr Lacey told the Commission that no victim certificates had been issued in Queensland until earlier this year, when iDcare assisted a victim to obtain one. The certificate is designed to be used by victims to restore credit ratings and counter other consequences of identity theft. It may be that little assistance can be obtained when the certificates are issued so long after the offence occurrence. In Queensland, certificates can only be issued upon conviction of an offender. By this time, a victim has already done much of what can be done to repair damage to their reputation. Although court-issued victims’ certificates are available across Australia, research conducted by the Australian Institute of Criminology suggests that victims are generally not aware of this recourse and/or see these certificates as being of limited utility.

Prevalence of organised crime and societal impacts

The crime types described above are likely to be perpetrated by syndicates or networks of offenders, often offshore, enabled by cybercrime. The Australian Cyber Security Centre, in their 2015 Threat Report stated:
Financially motivated criminals that exploit and access systems for financial gain are a substantial threat to Australia. Transnational serious and organised cybercrime syndicates are of most concern, specifically those which develop, share, sell and use sophisticated tools and techniques to access networks and systems impacting Australia’s interests.41

It is difficult to identify offenders, particularly as victims are not always immediately aware that their confidential information has been compromised. That often leads to a delay between the time of compromise and any report to financial institutions or law enforcement. Again, where financial data is stolen, reports are more likely to be made to financial institutions than to law enforcement. Thus, the impact of these crimes on Queensland residents and the economy is difficult to assess.

What is known is that card fraud not only causes financial inconvenience to individuals, but also causes harm to personal credit ratings, identity and privacy. The consequences might also extend to emotional stress and fears for personal safety.42

Further, while harming the banking sector in the first instance, the costs associated with card fraud are passed onto consumers of banking services. Commercial reputations also stand to suffer on account of this type of fraud, particularly where skimming and hacking has resulted in a successful breach of systems. There is no doubt that the threat of cyber-enabled fraud increases complexity and cost to businesses attempting to ‘balance the uptake of anti-fraud practices against other operational priorities.’43

A further difficulty with investigating—or even identifying—financial crimes is the low reporting rates to law enforcement. Victims of card data theft are often compensated by the financial institution to whom they have complained. While financial institutions are likely to keep records of their losses due to frauds, they do not necessarily forward those complaints to police. Other factors particular to victims of scams—involving shame and guilt—mean that those types of crimes are also under-reported.

In relation to financial crimes, QPS data is collected on five sub-categories of fraud:

- fraud by computer
- fraud by cheque
- fraud by credit card
- identity fraud
- other fraud

Statistics for those categories are generated from data input on the QPRIME database, by Policelink staff, and by police officers. Thus, data is reliant on accurate manual input, particularly in terms of which crime category is selected. Administrative staff and police officers are required to apply set procedures, in compliance with the National Crime Recording Standards.44 The QPS Operational Procedures Manual provides guidelines on how offences should be recorded. For example, multiple offences may have been generated relating to one stolen credit card, which is later used to purchase goods, but the occurrence will be recorded as one reported offence.

Mandatory reporting of data breaches by telecommunications companies and other organisations may further assist in combatting financial crime. Australian government agencies are required to report breaches, but publicly listed companies and those that store or process personal information are not.45 Proposed amendments to the Privacy Act 1988 (Cth) were introduced to Federal Parliament in 2013, to mandate reporting of certain data breaches. However, in 2014, a new bill was introduced without the mandatory reporting guidelines (Privacy Amendment (Privacy Alerts) Bill 2014 (Cth)). The Office of the Australian Information Commissioner provides a guide to handling personal information security breaches and strongly encourages organisations to report data breaches to promote good privacy practice. Although this requires federal intervention, the concept of mandatory reporting of data breaches is to put reputational (and financial) pressure on business to maintain effective cyber-security, thereby minimising both the likelihood and the impact of a data breach.46
Ultimately, most of the focus for these types of financial crimes has been on education and prevention. In relation to fraud and cybercrime in general, the QPS says it has taken a ‘proactive’ approach. The QPS Fraud and Cyber Crime Group (FCCG) has established Project Synergy, which has its foundations in education, increasing public awareness and partnering government, business and the community in an effort to manage and avoid cyber fraud.

Assessing the effectiveness of fraud prevention projects and community education is problematic, because it is not possible to measure the number of crimes not committed.

### 5.3.3 Scams

Many government agency websites warn consumers about current scams. Additionally, the ACCC ‘scamwatch’ website publicises common and reported scams, to educate consumers and prevent further financial crime.

The ACCC releases an annual report on scam activity. The 2014 report (Targeting Scams: Report of the ACCC on scams activity 2014) provides the following overview of where victims of scams are located:

<table>
<thead>
<tr>
<th>State</th>
<th>Percentage of total contacts that were based in Australia</th>
<th>Percentage of reported loss where contacts were based in Australia</th>
<th>Percentage of Australian Population*</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSW</td>
<td>31%</td>
<td>30%</td>
<td>32%</td>
</tr>
<tr>
<td>QLD</td>
<td>24%</td>
<td>24%</td>
<td>20%</td>
</tr>
<tr>
<td>VIC</td>
<td>22%</td>
<td>27%</td>
<td>25%</td>
</tr>
<tr>
<td>WA</td>
<td>9%</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>SA</td>
<td>8%</td>
<td>4%</td>
<td>7%</td>
</tr>
<tr>
<td>ACT</td>
<td>3%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>TAS</td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>NT</td>
<td>1%</td>
<td>0.5%</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>


### Advance-fee fraud and spam emails

Although scams and advance-fee frauds are not new, their reach is now extended by the Internet—targeting individuals who may never otherwise have been likely victims.

Advance-fee fraud generally refers to scams in which the recipient is required to pay fees in order to receive the prize which was the incentive to participate in the scam. They have also been commonly known as Nigerian scams because of the number originating from Nigerian syndicates, although they are no longer an exclusively Nigerian scam.

In the context of email scams, victims might respond to emails stating the recipient has:
- won a prize or a lottery
- been nominated as a beneficiary of a large overseas inheritance
- been selected as an appropriate person to receive an otherwise unclaimed windfall.

These scams can also be instigated through telephone, post or websites rather than unsolicited emails.

The prize is said to be somewhere offshore, and fees are required in order to send it internationally. For example, an anti-terrorist certificate might be required, at a cost of thousands of dollars. Each time the
Financial Crimes

Victims of such scams are often reluctant to make complaints due to a range of issues, including shame and embarrassment about being misled, and guilt about having brought others into the scam. When complaints are made, offenders based overseas are difficult to identify and prosecute. Recent media has highlighted secondary victimisation, where after having already been scammed of thousands of dollars, victims are then persuaded to travel to another country and return to Australia with illicit drugs (seemingly without their knowledge). As Detective Superintendent Brian Hay told the Commission:

What we had seen from a broader community impact perspective was that we had people that were self-funded retirees on private health care, with good health had now become dependent on the state for welfare, on the public hospital system and so many had attempted suicide, considered suicide and suffering depression. Some had committed other crimes to keep that dream alive, many had become isolated from their families and support networks… and the family resented them for spending the inheritance or legacy.

As demonstrated in the case study below, ‘victims’ may not realise or accept they are victims, particularly if they are deeply entrenched in the scam.

Case study

R v Malcolm Maiden

According to media reports, Maiden and his wife were invited to invest in a contract in the Nigerian oil industry in 2001. Over the following years, they sent over $2 million to accounts in Nigeria. From about 2005, the Maidens obtained loans from friends and associates to continue sending money in pursuit of the ultimate windfall promised them.

In 2006, the QPS Fraud and Corporate Crime Group (now known as the Fraud and Cyber Crime Group, or FCCG) undertook to identify victims who were sending cash to suspected Nigerian scammers. They were investigating the reasons why individuals in Queensland were sending money to Nigeria. The Maidens were identified as having sent several millions of dollars.

Police initially contacted the Maidens by telephone in early January 2006 and advised them that it was likely they were being defrauded. Police then attended in person in June 2006. Mrs Maiden indicated they would cease transferring money if their funds did not arrive in the coming fortnight.

QPS then identified that other persons were lending money to the Maidens. QPS again attended on the Maidens, in April 2007 (by which time they had sold their home and were living in a caravan). In May 2007, police attended again, this time with an investigator from the Nigerian Economic and Financial Crimes Commission cooperative. The Maidens were told that they were being defrauded and formally warned not to represent to others that the scheme was legitimate in order to borrow money.

However, the Maidens continued to seek assistance from their associates, and told one complainant that police and a Nigerian investigator had attended on them, and confirmed the legitimacy of the investment. A complaint was made to police in 2008, and the Maidens were charged with frauds relating to money borrowed after the warning had been given by police. The total amount defrauded by Mr Maiden was about $330,000. However, significantly more had been borrowed by him, prior to the warning being given by QPS.

Maiden declared bankruptcy in 2010. In 2011, he was sentenced in the District Court at Maroochydore on for five counts of fraud. Four counts included a circumstance of aggravation—that the amount defrauded...
was of a value of $5,000 or more. He was sentenced to a period of four years imprisonment, suspended after serving 12 months. Judge Robertson stated:

You’re obviously otherwise a man of good character. You became completely obsessed with this evil, fraudulent scheme, to the extent that even when you spoke to Detective Edwards, which I accept was a legitimate attempt by you to assist him in understanding the psychology that informs people who get involved in these schemes; even then, you were still a little bit hopeful that some money might come from it.

Mrs Maiden was sentenced in the Magistrates Court on 19 July 2010, to three years imprisonment with immediate release on parole.

In 2006 the QPS identified huge amounts of money being transferred by Australian citizens to Nigerian and other scammers. Since then there has been a focus on preventative education and providing support for victims. A victim support group meets monthly at the Brisbane Police Headquarters.

Between 2011 and 2014, QPS had an ‘advance-fee fraud portal’ which addressed, to some degree, the problem with directing complaints to the appropriate jurisdiction (in other words, where the offender resides). Complaints from Australian residents were able to be made directly to the Nigerian Economic and Financial Crimes Commission and the Ghana Police Service.57

The following case example demonstrates the transnational nature of these offences, both in relation to offenders and the victims. The scheme originated overseas, but an offender in Perth (the appellant) facilitated the scheme and provided some authenticity to it. Two complainants were based in Queensland, two in Victoria and one in Western Australia:

Case study

Nikaghanri v The State of Western Australia58

Nikaghanri was sentenced in the Western Australian District Court to an aggregate sentence of six years imprisonment for numerous fraud offences related to his involvement in ‘advance-fee fraud schemes’. The total amount defrauded was $132,429. He appealed the severity of his sentence to the Western Australian Court of Appeal. Leave to appeal was granted on two of three grounds of appeal. The appeal was dismissed on both grounds.

Complainants received emails advising that they had won a lottery, received a windfall as part of an estate, or had been selected as a suitable person to either look after funds owned by an army general or as an appropriate beneficiary of a large English estate with no beneficiary.

Complainants were told that certain payments needed to be made for transfer of the funds to Australia—for example, to obtain an anti-terrorist certificate. To complete the transfer, the complainants were put in contact with Nikaghanri, who used two false names. His conduct varied on each fraud, but generally he made promises and gave directions to convince complainants that progress was being made on the money that would finally be personally received by them.

The Court of Appeal quoted the finding of the sentencing Judge, who found that Nikaghanri was acting in concert with others:

[T]here was clear evidence that you were informed from time to time of the outline of a fictitious scenario being perpetrated on a victim in Australia. Your role was then to continue with that scenario … facilitating the final movement of promised funds to the expectant complainants, extricating fees from them for various fictitious governmental requirements and certificates.
Through collaboration with partner agencies, police can identify persons sending large amounts of money to countries considered to be suspect because of the number of scams identified as originating in those countries.

In 2006, the QPS commenced Operation Echo Track, after they became aware of a scam victim attempting suicide after losing a significant amount of money. At that time, there were no complaints of fraud in the Queensland Police Records Information Management Exchange (QPRIME) and no police intelligence that Queensland residents were being targeted or defrauded. Twenty-seven residents who had sent money to Nigeria were contacted and asked of their reasons for sending. Of those, 26 were considered to be victims of fraud, with a total amount in excess of $7.2 million. Further people were contacted, with 134 out of 139 identified as victims, totalling approximately $18 million. Since then, the QPS has intermittently undertaken approaches to potential victims, advising them of the scam and warning them against continuing to send money.

Transaction information comes from AUSTRAC, to whom all financial institutions and remittance providers are required to report suspicious transactions.

As described in the case study below, a partnership project between Western Australian Police and the Western Australian Department of Commerce uses the AUSTRAC data to investigate suspected scams and identify likely victims of advance-fee fraud:

### Case study

**Project Sunbird**

Western Australia’s Project Sunbird commenced in 2012 and targets five destination countries in West Africa. Transactions sent by Western Australians to those countries are identified. The investigation process is as follows:

1. Using financial intelligence, police identify potential victims and conduct a screening process. Unlikely victims are excluded (for example, genuine transfers made to family members), and a risk assessment is undertaken (for example, any risk associated with contacting the victim or identifying other criminal activity that the victim may be involved in).

2. The list of identified victims is then sent to the Department of Commerce. A letter is sent to the victim identifying the potential fraud and providing contact details for a Project Sunbird staff member.

3. The Department of Commerce interrupt payments by blocking accounts and educating victims.

4. Police and the Department of Commerce combine to gather information from letter recipients.

5. From the information gathered, police investigate local offenders, if identified, or make referrals to overseas law enforcement.

High-risk victims are those who have transferred large amounts, those who could be unwittingly money laundering or those who have planned international meetings with the perpetrator. Home visits or face-to-face contact appointments are organised for those victims assessed as high-risk.
Analysis of the project by academicians identifies the following benefits:60

- The project provides more accurate data on fraud crime, including amounts of money and number of victims.
- Incident reports created by police may lead to better resourcing and an increase in funding, given that most resourcing budgets are determined based on offence-reporting statistics.
- Upon receiving a letter, 66 per cent of people stop sending money and 14 per cent reduce how much they send, but if they continue to send money or there is an increase in how much is sent, data suggests that upon receipt of a second letter, 44 per cent stop and 33 per cent decrease the amount sent.
- The project provides assistance to other law enforcement agencies inside and outside of Australia to arrest those responsible for perpetrating online fraud.61
- The project provides monitoring of accounts of known offenders to identify other victims.

The research undertaken has limitations. For example, it is not known how many persons and how much money is sent to countries other than the five identified in the project. Analysis of the long-term benefits and sustainability of such a project may be required.62

A problem encountered in trying to stop victims sending money is that having already invested (and lost) so much of their savings, victims are entrenched in the scam and may be reluctant to both abandon the belief that promises will be fulfilled and accept they have been defrauded. Those victims continue sending money, even after being warned of the fraud, as in the case example of R v Malcolm Maiden discussed above. The best time to convince victims to cease sending money is when they have invested only a small amount—usually at the beginning of their involvement in the scam. A criminologist researching victims of online fraud has stated that ‘the best strategy is to proactively identify victims at the earliest possible stage of their participation in a fraud’.63

While there is no current project identifying victims of advance-fee fraud, the QPS FCCG continues to receive and analyse data from AUSTRAC, and have an AUSTRAC officer embedded in their team.

Romance/social-networking scams

Primarily, romance/social-networking scams involve the grooming of victims in the context of developing a relationship online via dating websites or social networking sites. Having fraudulently established a relationship, the offender then persuades victims to send money on false premises. Occasionally, victims are used to unwittingly launder dishonestly obtained cash.

Dating or social networking scams usually involve victims paying fees to be a member of the website, without ever receiving any goods or services for the fee, or being required to make continuous fees to keep communicating with a prospective partner, who does not actually exist (in other words, pay for each email sent and received).64 The ACCC recently reviewed 65 online dating websites for compliance with the ACCC’s Best Practice Guidelines for dating websites and the Australian Consumer Law, with findings detailed in the Online dating industry report published 12 February 2015.65 However, the Commission focused on romance scams, given that there is some evidence that organised, international syndicates perpetrate these scams in a similar way to advance-fee frauds.

Romance scams perpetrated by organised crime traditionally originated in West African countries like Nigeria and Ghana, but it is now believed that perpetrators are located around the globe.66 Scams commonly use images of real people, such as attractive models or United States army officers. Fake online profiles are created relying on those images.

Given that the images are of real people, identity theft facilitates the romance scam. For example, United States Army three-star Lieutenant-General William B. Caldwell IV has had thousands of women fall in love with him, without having ever met him: ‘[H]is image has been misappropriated thousands of times by fraudsters from Nigeria, Ghana and other places’.67 Despite being happily married, information on his
Wikipedia page is often changed to describe him as a widower. His secretary handles numerous calls from women around the world, who believe that he is the man they fell in love with. He has retired now, but on one day alone in mid-November 2014, 23 fake profiles using his last name and photos were removed by his IT team.

A Queensland woman, who fell in love with him, described receiving Skype requests to chat with him online soon after she retired from the public service:

She ignored them until his birthday, when she felt sorry for the soldier spending his birthday in a war zone. Over the next five months, the imposter, very likely a Ghanaian business syndicate of men and women, convinced her to give $130,000 to a cast of characters ranging from a French banker to an African diplomat who said they were bringing money to fund their version of happy-ever-after.

An ‘anatomy of the scam’ or the ‘scammers persuasive technique model’, as formulated by academic research conducted in the United Kingdom, can be summarised as follows:

1. Victim is motivated to find love/the ideal partner.
2. Victim is presented with the ideal profile (fake profile created).
3. Grooming process: scammer quickly declares love and requests the relationship move to instant messenger and email; trust gained; frequent and intense communication online (limited telephone contact).
4. The sting: scammer may request gifts to test the water; scammer then requests small amounts of money; stakes are raised with larger sums requested on the pretense of some crisis occurring (or some variation of the three—some scammers may not test the waters, others may only ask for small amounts of money over a long period of time).
5. Continuation of scam until victim runs out of money, exits the scam or learns that they have been scammed; further crises presented with larger sums requested; other characters may be brought into the narrative; ‘a ‘doctor’ might contact the victim telling them their loved one is in hospital’.

Some scammers have employed sexual abuse/blackmail (also known as ‘sextortion’) by requesting their victim to conduct a sexual act by webcam, with the victim later blackmailed with the threat of dissemination of the video. Further, some targets are re-victimised after learning of the scam by, for example, the scammer admitting to the scam but professing to have genuinely fallen in love with the target, or when another person contacts them claiming to be law enforcement and asking for a fee to release their stolen funds.

The narrative adopted by scammers depends on the gender of the target:

- Male fictitious characters often start off wealthy in high status positions (e.g., army general, business owner, man[ager] of a big company). They might have lost their wife in a tragic accident and are sometime[s] left with a child to care for. Female characters are often young and vulnerable. They have a job, but not typically of high status (e.g., a nurse or a teacher).

Targets have been persuaded to visit an African country where they risk being kidnapped, or becoming involved in other illegal activities such as money laundering.

In February 2013, a Western Australian woman, Jette Jacobs, was found dead in South Africa under suspicious circumstances. She had travelled to South Africa in November 2012 to meet a Nigerian man, whom she had met online four years earlier. She had travelled to Johannesburg and met him in 2010 without incident. Over the course of the four years, she had transferred approximately $80,000 to him. She was identified as a potential victim through Western Australia’s Project Sunbird, but their initial letter arrived after she had already left Australia.

The only known case in Queensland of a person actively involved in a romance/advance-fee fraud is that of Shirley La Ragy, who was sentenced in the District Court at Rockhampton on 15 November 2011 for her involvement in a scam. She defrauded five men of approximately $590,893.82. All men were citizens of the United States or Canada. Ms La Ragy created false female profiles on Internet dating sites, then made
promises to the men in the context of romantic relationships. The men sent large amounts of money to Ms La Ragy’s account. She then forwarded the money to other criminal participants in Nigeria. She had been encouraged to participate after commencing a relationship with a Nigerian man in 2005.78

As reported by the ACCC in the February 2015 Online dating industry report, dating and romance scams account for over 30 per cent of total reported scam losses, with those reported losses being the highest of any scam category. While clearly prevalent, it is difficult to assess the extent that it is perpetrated by organised crime rather than by individuals.

The Scam Disruption Project, implemented by the ACCC, identifies and contacts consumers to advise them that they may be a victim. The ACCC states that disrupting relationship scams is a priority, because of the potential devastating emotional consequences for a victim.79

The ACCC’s 2014 report (Targeting Scams: Report of the ACCC on scams activity 2014) shows that dating/romance scams account for the greatest loss to Queensland complainants, in the order of $5.8 million.80

<table>
<thead>
<tr>
<th>Scam Category Level 2</th>
<th>Amount reported lost</th>
<th>Contacts reporting loss</th>
<th>Contacts reporting no loss</th>
<th>Conversion rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dating and romance</td>
<td>$5,780,010</td>
<td>544</td>
<td>234</td>
<td>147</td>
</tr>
<tr>
<td>Investment schemes</td>
<td>$3,007,622</td>
<td>186</td>
<td>76</td>
<td>29</td>
</tr>
<tr>
<td>Computer prediction software and sports investment schemes</td>
<td>$2,511,220</td>
<td>111</td>
<td>60</td>
<td>14</td>
</tr>
<tr>
<td>Nigerian scams</td>
<td>$797,252</td>
<td>251</td>
<td>18</td>
<td>11</td>
</tr>
<tr>
<td>Other buying and selling scams</td>
<td>$739,094</td>
<td>1633</td>
<td>556</td>
<td>536</td>
</tr>
<tr>
<td>Classified scams</td>
<td>$661,815</td>
<td>823</td>
<td>159</td>
<td>140</td>
</tr>
<tr>
<td>Hacking</td>
<td>$647,297</td>
<td>936</td>
<td>72</td>
<td>68</td>
</tr>
<tr>
<td>Other upfront payment and advanced fee frauds</td>
<td>$528,360</td>
<td>941</td>
<td>128</td>
<td>118</td>
</tr>
<tr>
<td>Ransomware and malware</td>
<td>$506,590</td>
<td>566</td>
<td>32</td>
<td>27</td>
</tr>
<tr>
<td>Other business employment and investment scams</td>
<td>$505,984</td>
<td>194</td>
<td>45</td>
<td>33</td>
</tr>
<tr>
<td>Remote access scams</td>
<td>$544,403</td>
<td>1813</td>
<td>182</td>
<td>174</td>
</tr>
<tr>
<td>Unexpected prize and lottery scams</td>
<td>$272,501</td>
<td>696</td>
<td>57</td>
<td>52</td>
</tr>
<tr>
<td>Inheritance scams</td>
<td>$239,625</td>
<td>1036</td>
<td>14</td>
<td>6</td>
</tr>
<tr>
<td>Fake trader websites</td>
<td>$215,831</td>
<td>397</td>
<td>257</td>
<td>252</td>
</tr>
<tr>
<td>Job and employment</td>
<td>$210,473</td>
<td>435</td>
<td>45</td>
<td>43</td>
</tr>
<tr>
<td>ID theft involving spam or phishing</td>
<td>$183,087</td>
<td>1750</td>
<td>95</td>
<td>89</td>
</tr>
<tr>
<td>Hitman scams</td>
<td>$150,728</td>
<td>60</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td>Overpayment scams</td>
<td>$138,744</td>
<td>361</td>
<td>38</td>
<td>35</td>
</tr>
<tr>
<td>Pyramid schemes</td>
<td>$122,285</td>
<td>50</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Scratchie scams</td>
<td>$102,586</td>
<td>137</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>Fake charity scams</td>
<td>$96,489</td>
<td>169</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>Reclaim scams</td>
<td>$89,471</td>
<td>3979</td>
<td>48</td>
<td>47</td>
</tr>
<tr>
<td>Phishing</td>
<td>$77,372</td>
<td>2801</td>
<td>71</td>
<td>69</td>
</tr>
<tr>
<td>False billing</td>
<td>$50,660</td>
<td>653</td>
<td>71</td>
<td>71</td>
</tr>
<tr>
<td>Travel prize scams</td>
<td>$18,703</td>
<td>371</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Mobile premium services</td>
<td>$12,497</td>
<td>60</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>Health and medical products</td>
<td>$10,034</td>
<td>91</td>
<td>46</td>
<td>46</td>
</tr>
<tr>
<td>(blank)</td>
<td>$5,637</td>
<td>161</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Psychic and clairvoyant</td>
<td>$865</td>
<td>15</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>$18,025,235</td>
<td>21,220</td>
<td>2408</td>
<td>2111</td>
</tr>
</tbody>
</table>
Unfortunately, those lured into romance scams may not readily accept that they are victims of a scam. Having invested so much emotionally—and financially—into the often long-term relationship, it can be difficult for victims to face the reality of the scam, even when presented with overwhelming evidence. The following example appears to involve an individual scammer, but demonstrates the societal and financial impact of the romance scam no matter how many scammers are involved:

**Case study**

*FAJ*°\(^81\)

FAJ’s son brought an application in the Queensland Civil and Administrative Tribunal (QCAT) seeking the appointment of an administrator and a guardian for FAJ, essentially to prevent FAJ from sending money to a person (PM) in the United States, with whom she had developed an online relationship. FAJ’s family and friends were concerned that she had sent large amounts of money to PM, even after being presented with evidence suggesting that she was victim of a scam.

FAJ was widowed in 2009. Her estate included her principal place of residence, an investment property and several other cash and shares investments. FAJ met PM in 2010, through an Internet poker site. FAJ and PM had never met in person, but had exchanged regular electronic communications and telephone calls.

Between June 2011 and August 2013, FAJ ‘loaned’ PM significant amounts of money. She sold her investment property in June 2012. Funds equivalent to the sale were sent to PM within two months.

By June 2013, FAJ was unable to pay body corporate fees and council rates on her residence. She had reached the maximum limit on her credit cards. FAJ asked friends for loans to pay her bills and also made unsuccessful finance applications at three major banks. FAJ told one bank’s lending specialist that the money was for ‘personal use to send overseas’.°\(^82\) In mid-July 2013, FAJ put her residence on the market.

Her son intervened, and the sale proceeds were invested in a high-interest account, pending the outcome of the QCAT proceeding.

FAJ continued to be in love with PM, believing him to be genuine. She believed him to be single and, believing they would soon marry, she had made preparations for his imminent arrival in Australia to live with her. She maintained that three ‘promissory’ notes provided by him demonstrated he would repay the borrowed funds. She gave numerous reasons why PM needed money, including that he had done legal work for the mafia and had borrowed from them at a high interest rate, and that he had lost money after the death of a wife and in educating his children.

The QPS Fraud Squad and the Federal Bureau of Investigation (FBI) in the United States provided assistance to FAJ’s family. The FBI interviewed PM in August 2013. PM said most of the loaned money was spent on gambling slot machines, although some was used to pay off gambling debts. He said he planned to pay FAJ back with future gambling winnings. He described himself as a professional gambler. There was evidence that PM had a history of failed businesses and bankruptcy in Canada and a criminal record in the United States—including arrests for deceptive practices, computer fraud, theft, and impersonation.

Information strongly suggested PM to be married and living with his wife in a jointly owned property. In November 2013, PM claimed that the co-habitation with his wife was only an arrangement to allow him to live in the United States.

The promissory notes did not offer reasonable (if any) security for the large sums of money involved. The large amounts loaned significantly changed FAJ’s life—she went from living in comfortable circumstances in 2009 to living in rented premises with very limited income and a significantly deficit budget in 2013.°\(^83\) Unless restitution of her capital funds was made, FAJ faced ongoing and permanent deterioration in her standard of living.°\(^84\)
The proceeding caused stress and anxiety to FAJ, in light of her continued affection for PM. Further, the loans not only caused financial hardship for her, but also caused damage to her relationships with her children and friends. About her son, Member Bayne stated:

... LR in particular has gone to extraordinary and well justified lengths to protect his mother and her assets and to produce reliable evidence. He is clearly not motivated by any self-interest, and shows genuine and considerable concern for the wellbeing of his mother.85

Member Bayne determined that FAJ had impaired decision-making capacity for financial, personal and health matters, despite the there being no underlying broad category of disability to explain the incapacity.86 An order was made that the Public Trustee of Queensland be appointed as administrator for FAJ for all financial matters. A guardianship order was not made.

At least two Queensland academics (Dr Cassandra Cross and Dr Jacqueline Drew) have worked with QPS in the area of scam victims. Dr Cross worked as a research and policy officer with QPS for five years, and in 2011, through the Donald Mackay Churchill Fellowship, studied methods for preventing—and supporting victims of—online fraud. In 2014, Dr Jacqueline Drew conducted a research project with the QPS FCCG, focusing on online fraud and the factors ‘likely to be most effective in disengaging individuals from participation in a fraud’.87

There are many factors that contribute to targets becoming victims, but one factor, which may be peculiar to the online romance scam, is that the scammer professes to live abroad—thus avoiding the typical process of meeting quickly after initial contact on an online dating site.88 This gives the scammer time—and therefore knowledge—to present an ideal person to the victim.89 The scammer creates a strong attachment by making the relationship become part of the daily routine. Romantic messages can be reinforced through repetitive viewing by the target, which does not occur face-to-face. Those factors combine to create a ‘hyper-personal’ relationship, from which it is difficult for victims to break away.90

The consequences of such scams is not solely financial. Victims often feel shame, embarrassment, guilt, anger and fear, and in the process of persisting with the relationship, may have become estranged from loved ones who attempted to intervene.

Across the gamut of financial crimes where individuals are concerned (as opposed to financial institutions), a significant problem for victims is the perception that their victimisation was a result of either stupidity or greed. This often means little focus is placed on the offender, particularly where the offender is faceless and located offshore. It can also leave victims feeling powerless and less inclined to report crimes to police.

Scams in particular leave victims at risk of suicide and self-harm. As reported in the media, a Queensland interior decorator attempted to commit suicide twice due to shame and despair at losing $300,000 to a Nigerian email scam.91 Although there is a paucity of research study on fraud victims, some findings suggest that victims ‘share many of the same devastating outcomes as their counterparts who have suffered serious violent crime’.92 The harm suffered is not exclusively financial, and can include emotional/psychological trauma and relationship breakdowns.93

(Endnotes)


16 Transcript of Interview, David Lacey, 2 July 2015, pp. 9–10.


24 R v Tovt (Unreported, District Court of Queensland, Clare SC DCJ, 20 August 2014).

25 R v Stroia [2011] QCA 317; R v Stroia (Unreported, District Court of Queensland, Martin DCJ, 27 February 2015); R v Tovt (Unreported, District Court of Queensland, Clare SC DCJ, 20 August 2014); R v Gautum (Unreported, District Court of Queensland, Ryrie DCJ, 24 April 2014).

26 R v Jenkins (Unreported, District Court of Queensland, Martin SC DCJ, 7 January 2014).

27 Statutory declaration, Terry Lawrence, 20 August 2015, para 4, p. 2.

28 Statutory declaration, Terry Lawrence, 20 August 2015, para 5, p. 2.

5 Financial Crimes


R v Gordeev (Unreported, District Court of Queensland, Dearden DCJ, 8 February 2006).


Transcript of Interview, David Lacey, 2 July 2015.


Transcript of interview, Brian Hay, 19 June 2015.

R v Maiden (Unreported, District Court of Queensland, Robertson DCJ, 7 March 2011).


R v La Ragy (Unreported, District Court of Queensland, Koppenol DCJ, 15 November 2011).


FAJ [2013] QCAT 703.

FAJ [2013] QCAT 703, footnote 6, p. 4.

FAJ [2013] QCAT 703, p. 11.

FAJ [2013] QCAT 703, p. 11.


FAJ [2013] QCAT 703, p. 15.


5.4 Related activities

5.4.1 Cyber and technology-enabled crime

It is abundantly clear that cyber and technology-enabled crime is now a common thread through all types of financial organised crime. Gone are the days when the greatest risk of financial data theft or identity theft was through an unlocked footpath mailbox. Cybercriminals are now able to hack electronic devices, harvest personal details, embed malware and ransomware, and launder money by trading virtual currencies on the Darknet, all with the assistance of anonymising services to help avoid detection.

Like identity crime, cyber and technology-enabled crime not only enables other types of crime, but is also a crime type in itself. There is a dedicated Cyber and Identity Crime Investigation Unit within the QPS Fraud and Cyber Crime Group (FCCG).

In the financial crime context, cyber and technology-enabled crime has the potential to cause severe harm to individuals as well as to broader Australian interests. Those harms include damage to personal identity, reputation and/or credit rating, as well as the loss of business or employment opportunities. There are often significant consequences to emotional and psychological wellbeing.

There is no doubt that the greatest challenges to law enforcement agencies in the modern age flow from the evolving opportunities exploited by criminal networks in the cyber environment.

5.4.2 Identity crime

At the core of financial data theft, there is often a compromise or misuse of identity information. Consequently, the two crime types (financial data theft and identity crime) are intimately linked. In 2007, the Australian Federal Police’s Response to the Model Criminal Law Officers’ Committee Discussion Paper – Identity Theft stated that at the time, identity crime was arguably the fastest-growing crime around the world.

The Australian Institute of Criminology’s research on identity crime uses the broader concept of ‘misuse of personal information’. In their most recent general survey relating to identity crime, approximately 20 per cent of 5,000 respondents had experienced some misuse of personal information in their lifetime, whereas only four to five per cent of respondents experienced other offences in their lifetime.1
In the context of increasing concerns about identity crime, the Council of Australian Governments in 2007 formulated an *Intergovernmental Agreement to a National Identity Theft Strategy*. That strategy has since been reviewed and updated to ensure its currency, resulting in the *National Identity Security Strategy 2012*.

Numerous definitions have been generated around identity-related crime, both nationally and internationally. The following definitions, formulated in 2006 by the Australasian Centre for Policing Research, were endorsed by the above-mentioned 2007 Council of Australian Governments agreement:

- **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime.

- **Identity fraud** is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.

- **Identity theft** is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased.

Using those definitions, identity refers to both individual and corporate identities, and incorporates the manipulation or assumption of part of an identity. Organised crime is facilitated by identity crime—allowing offenders to hide their true identities and avoid detection.

It is estimated that across Australia, direct losses from identity crime exceed $1.5 billion per year, with further costs expended investigating and prosecuting those crimes. The Australian Crime Commission (ACC) reports that assessment of the extent of identity crime is limited by:

- its cross-jurisdictional nature, and related determinations of the jurisdiction in which the offence has been committed
- the varying legislation across police jurisdictions, as well as the use of other offences such as fraud to prosecute offenders
- the lack of reporting by victims (who may not be aware of the compromise or who may report it to a financial institution rather than police)
- reluctance by businesses to report it, to avoid loss of confidence in the business
- later use of stored information, making it difficult to identify the original breach source and time
- the use of identity crime to support more serious criminal activities, making measurement of harm from the identity crime difficult.

In 2014, two offenders in Queensland were prosecuted for using high-level forged identity documents to successfully obtain loans and credit cards from financial institutions. Both offenders maintained that they were working within a syndicate, although collateral evidence of the syndicate was not placed before the sentencing courts.

**Case study**

**R v Mahmut Baity (DPP Schedule of Facts)**

Baity was involved in an organised scheme. He obtained fake documentation, including forged Victorian Drivers Licenses and a Medicare card. He obtained and used false payslips from fictitious companies, including one which had been registered with the Australian Securities and Investment Commission. A bank became suspicious and reported him to police. He participated in a record of interview, where he told police that he had been given instructions and the forged documentation by another person, to whom he gave half the money.
Case study

R v Andreou (Unreported judgement)

Andreou committed a number of frauds over several years, including frauds committed using the eBay bidding system (people made successful bids for products but the product was never received). Notably, over a 10-month period between 2011 and 2012, he obtained credit cards from Westpac Bank under nine different fraudulent names, and drew down approximately $170,000. He maintained that he was working at the direction of accomplices.

When police executed a search warrant on Andreou’s residence, they located numerous computers, printers and identification products, including images of Mahmut Baity.

As well as actual crime committed to obtain identity information, identity crime enables other financial crimes—and is linked to major crimes such as drug trafficking, people smuggling, and money laundering. In a cold-call investment fraud, false company identities are created—or existing company information manipulated—to persuade victims of the authenticity of the investment scheme. Offenders have registered business names similar to an existing, established company, making it harder for consumers to conduct due diligence.

Identity crime is also a key enabler of superannuation fraud. Price Waterhouse Cooper’s 2012 Global Economic Crime Survey reports that crime syndicates have been targeting Australian superannuation funds. The report identifies the key risks to superannuation funds as including identity fraud (where syndicates use fake identification to create self-managed super funds and then withdraw customer savings), false death certificates, and phishing scams, as well as professional facilitators (such as financial planners, accountants and advisers) diverting funds.

The following case study demonstrates the use of identity theft to target superannuation accounts.

Case study

AUSTRAC investigation of superannuation fraud

Syndicate members stole cheques, superannuation statements and personal bank statements from mailboxes. This information was used to produce high-quality counterfeit identity documents, which were, in turn, used to conduct frauds. Some victims were approached directly.

The fraud methods included:

1. Using the identification to open a self-managed superannuation fund (SMSF) in the victim’s name, and then linking a fraudulently obtained bank account using the details of the new SMSF. Assuming the victim’s identity, a request is made for the victim’s superannuation provider to ‘roll over’ funds from the legitimate superannuation fund into the fraudulent SMSF. Funds are then withdrawn from the new SMSF account and sent offshore using remittance service providers.

2. Victims are offered the chance to access superannuation funds early. Common targets are people struggling with debt, those who are unemployed, and people from non-English speaking backgrounds. Enticed by the offer, the victim provides financial and identification details to facilitate the early release of funds. Funds are withdrawn, with about 20 per cent taken by the syndicate as a fee and the balance paid to the victim. Alternatively, the syndicate steals all the victim’s funds and the victim receives nothing.
3. Victims are told of a better return on their superannuation, if they roll it over into a legitimate fund. Once their financial and identification details are provided, the syndicate rolls the funds into the syndicate member’s fraudulent SMSF and withdraws the funds from the bank account.

AUSTRAC received suspicious matter reports (also known as ‘SMRs’) and suspect transaction reports (also known as ‘SUSTRs’), and through information in the reports and further analysis, identified a large criminal syndicate. One particular suspicious matter report identified a syndicate member as the signatory to two new business cheque accounts, opened to operate two SMSFs. Over three months, the accounts received over $500,000, rolled from several superannuation funds. Once deposited, the funds were immediately withdrawn. International transfer information was reported to AUSTRAC by reporting entities. According to the AUSTRAC typologies report:

A total of 25 syndicate members were charged with over 2,500 offences involving the laundering of over AUD8 million in fraudulently obtained funds. The head of the syndicate, who controlled three bank accounts which turned over AUD1.6 million, was charged and found guilty of 57 counts of identity fraud and money laundering relating to transactions valued at more than AUD550,000.⁹

Many government agencies and businesses now warn consumers about identity crime and how it is committed. For example, the Australian Taxation Office website contains information about protecting personal information and the impact of identity crime on both individuals and businesses.¹⁰

5.4.3 Professional facilitators

Insofar as financial crime is concerned, the following professional facilitators are particularly relevant:

- accountants and financial advisers
- lawyers
- real estate agents
- IT professionals and technical security experts

Additionally, other service providers are considered to enable cold-call investment frauds, because they are used to provide authenticity to the investment scam promoted by the offenders (see below).

Remitters (persons/entities who transmit money, such as Western Union) are also considered to be enablers of financial crimes to the extent that perpetrators of organised financial crime often use remittance services to transfer ill-gotten gains overseas, where there is a transnational element (for example, advance-fee frauds and skimming syndicates). Further discussion of the role of remitters in laundering funds is explored in the chapter on money laundering.

The extent that professional facilitators provide assistance to organised crime remains largely unknown:

Although law enforcement and regulators continue to find evidence of the use of both simple and complex business structures and illegal business practices to facilitate criminal activity and to hide the proceeds of crime, the full nature and extent of organised crime involvement remain an intelligence gap.¹¹

Often, professionals may unwittingly facilitate the commission of offences. However, the ACC also explains that:

In an era of an increasingly competitive business market, legitimate companies and individuals may switch to unethical practices to survive. Providing services to criminal groups may be an attractive source of income. Criminal networks are skilled in identifying these weaknesses.¹²
The same ACC publication lists the following examples of the types of work that professionals may provide to organised crime:

- laundering money by working around regulations and controls in the regulated financial sector, or by buying or selling high-end luxury goods
- manipulating import processes at borders
- transporting and storing illicit goods
- assisting with technical components in manufacturing illicit drugs
- reaching and communicating with intended victims of fraud
- providing access to communication facilities such as phone, fax or email so criminal groups can communicate with each other using the facilitator’s business as a ‘shield’
- helping criminals avoid detection when laundering money by adding legitimacy to financial transactions
- providing clandestine accommodation for human trafficking victims
- using computer technology to help steal identities.

The Commission found no evidence of any of the described activities having been knowingly performed by professional facilitators in Queensland. The Commission knows only of two solicitors who have been charged (but not convicted) for conduct related to structuring to avoid reporting obligations under the Anti-Money Laundering/Counter Terrorist Financing Act (AML/CTF Act).

A recurring theme throughout this Inquiry has been the importance and benefit of information-sharing between the private sector, regulatory bodies, and law enforcement. Here, information-sharing between law enforcement and agencies responsible for professional regulation may assist in identifying and preventing facilitation of organised crime.

Accountants and financial advisors

Accountants and financial advisors may be involved in organised crime by facilitating illegal tax avoidance schemes. For example, in 2013, a qualified accountant based in Geneva was convicted in the Brisbane Supreme Court of three counts of conspiring to defraud the Commonwealth.

No single body is responsible for regulating the accountancy profession in Australia, or Queensland. Accountants can obtain membership of one or more of three representative bodies:

- Chartered Accountants Australia and New Zealand (CAANZ) – formerly the Institute of Chartered Accountants Australia (ICAA)
- CPA Australia (CPA) is the abbreviation for Certified Public Accountant
- Institute of Public Accountants (IPA).

Each body regulates its members and takes disciplinary action where misconduct is investigated and substantiated. Accountants apply for membership, which may be offered at varying levels. Generally, payment of a fee is required and certain pre-requisites must be met (such as completion of specified courses). Membership of a representative body is not mandatory to practice as an accountant. However, consumers generally seek accountants who have membership of one of the three recognised bodies, and employment by large firms is usually contingent on membership in one of the representative bodies.

There is no external regulation of accountants. Each representative body has a disciplinary arm that investigates complaints and may refer practitioners to a tribunal. Practitioners who breach the standards set by the representative body can face suspension of—or exclusion from—membership. Suspension does not preclude continued work as an accountant; however, in a practical sense, employment is restricted because the member can no longer practice as an accountant with the designated membership.
All three accounting bodies are members of the Accounting Professional and Ethical Standards Board, which issues a Code of Ethics for Professional Accountants (APES 110), based on international ethics standards for accountants. Practicing members must observe and comply with this Code (paragraph 100.1). Although the Accounting Professional and Ethical Standards Board issues standards of professional conduct, each accounting body is responsible for their enforcement and for disciplinary action of members who breach the Code.

The Chartered Accountants Australia and New Zealand disciplines members who breach its by-laws, regulations and the APES 110 and thereby discredit the profession or harm the protection of the public interest. The organisation has program regulations and a candidate code of conduct.

The Institute of Public Accountants sets professional and ethical requirements for members through its constitution and by-laws, and as promulgated by its board of directors or by the Accounting Professional and Ethical Standards Board. It issues standards in conjunction with those issued by the Accounting Professional and Ethical Standards Board (in other words, the APES 110). The constitution and by-laws empower it to enforce observance of those standards.

Membership of CPA Australia requires compliance with its constitution and by-laws, the code of professional conduct and applicable regulations. The constitution states that the code of professional conduct refers to the APES 110.

All three bodies set standards of professional conduct that essentially adopt APES 110 and broadly promote best practice. Application of the guiding principles in APES 110 by accountants could be apt to deter involvement in enabling organised crime. The consequences of a breach can be severe, in that serious breaches result in forfeiture of membership for a period of time, with a consequence that an accountant’s employment may be lost. Each body has an application process where an accountant seeking membership would be required to disclose a previous disciplinary proceeding. Investigations of misconduct seem often to be triggered either by a client complaint or an investigation by a regulatory or law enforcement body—that is, after the misconduct has already been identified elsewhere. At times, no further disciplinary action is taken by the accounting body, having regard to penalties imposed in other forums.

Each of the three representative bodies were asked to provide a submission to the Commission. None were forthcoming. The Chartered Accountants of Australia and New Zealand did advise the Commission that there was nothing their organisation could add to the Commission’s consideration of the Terms of Reference.

**Lawyers**

Lawyers are routinely included in the list of professionals who may be facilitating organised crime. However, very little has been written about specific instances of involvement, or about the extent or prevalence of such involvement, other than in relation to money laundering (see the chapter titled Money laundering, below).

The Australian Crime Commission considers that professional facilitators may be enabling the criminal exploitation of business structures, particularly in relation to laundering proceeds of crime, but also in other areas:

- This may be through the exploitation of simple and complex business structures, through the practice of fraudulent phoenixing, and increasingly with the support of professional facilitators who have the expertise to navigate through complicated business practices and arrangements in order to conceal illegal activities and avoid detection.

Additionally, the ACC reported that ‘Project Wickenby investigations uncovered the abuse of complex legal structures involving chains of company ownership, trusts and other corporate entities to hide the true ownership of funds for tax evasion purposes.’

The Victorian Law Reform Commission grouped lawyers, accountants and financial advisers together because they are said to perform the following ‘broadly similar enabling tasks’:
• advising on and implementing complex business structures in order to conceal real ownership of businesses used for criminal activity and/or to launder the proceeds of crime (including the establishment of overseas entities)
• advising on the circumvention of anti-money laundering legislation
• managing investments, including intermingling the proceeds of crime with legitimately acquired funds in investments such as securities, legitimate businesses and real estate
• advising on fraudulent tax arrangements (including tax evasion measures and the fraudulent claiming of tax concessions)
• advising on the operation of fraudulent, high-yield investment schemes by organised crime groups and/or referring clients into such schemes. Fraud and financial crime is an increasingly common form of activity by organised crime groups.

AUSTRAC, in their strategic analysis brief entitled, Money laundering through legal practitioners, describe the ‘vulnerabilities associated with legal practitioners’ as follows:

The types of services provided by legal practitioners make them attractive for money laundering. Legal practitioners can play a key role in providing advice and services that assist criminal groups with establishing legal, corporate and financial structures to launder illicit funds.

Legal practitioners provide a veneer of legitimacy. The professional status of legal practitioners enhances the legitimacy of transactions and financial activity, and correspondingly reduces the risk of such activity raising suspicion.

Although it is likely that lawyers in Queensland are facilitating organised crime in at least some of the ways outlined by the ACC, the Victorian Law Reform Commission and AUSTRAC, the Commission found no reported cases. As previously mentioned, two solicitors were charged earlier this year with structuring offences under the AML/CTF Act. Those matters are currently the subject of judicial proceedings, and, in accordance with the Terms of Reference, the Commission must not have regard to them.

Solicitors are required to comply with the Australian Solicitors Conduct Rules, which set out the ethical guidelines for practice. In Queensland, solicitors take membership of the Queensland Law Society, but complaints about solicitors are investigated by the Legal Services Commissioner. If investigations indicate that solicitors have engaged in ‘unsatisfactory professional conduct’ or ‘professional misconduct’, the Legal Services Commissioner will commence an action against the solicitor in the Queensland Civil and Administrative Tribunal (since 2009), with rights of appeal for both parties to the Court of Appeal. The Legal Services Commissioner maintains a register of published decisions in relation to discipline applications it has made. Many disciplinary proceedings involve conduct associated with trust accounts.

The potential extension of the AML/CTF Act reporting obligations to accountants and lawyers is likely to be met with resistance by professional bodies representing both groups. The concern regards the impact of the reporting obligations on the fundamental duties of confidentiality central to client relationships in both professions.

Real estate agents

Links may exist between financial crime and real estate agents, although the Commission found no evidence of this in the last three years. Real estate agents have been identified as ‘high risk’ in relation to money laundering (again, see the chapter titled Money laundering, below). Despite the industry’s high-risk status, it remains unregulated by the AML/CTF Act.

In order to address the risk of real estate agents wittingly or unwittingly facilitating identity fraud and industry scams, both New South Wales and Western Australia have strengthened, through guidelines, verification of identity requirements. Additionally, in South Australia and Western Australia, any lawyers, conveyancers and mortgagees conducting conveyance transactions are required to visually verify the identity of certain persons involved in real estate transactions.
Guidelines were developed after two incidents in 2010 and 2011, where properties were sold in Western Australia without the knowledge or consent of the lawful property owners. The 2011 fraud involved the sale, apparently by Nigerian scammers, of a couple’s home in Perth while they were living overseas. A real estate agent was contacted by a man claiming to be the owner and asking that the agent effect an urgent sale of the property. The earlier fraud was very similar.

**Verification of identity – real estate agents**

In Western Australia, a guidance note for real estate agents regarding client identification verification and real estate fraud prevention amends the statutory real estate agents’ code of conduct by requiring agents to conduct a ‘100 point check’ client identity verification. Further, the note recommends face-to-face identity verification as standard practice, with agents to sight original documents to verify identity wherever possible. Where such contact is not possible, the agent is to ensure that documents provided for the check are sighted and verified as a true copy of the original, by a suitable independent and verifiable witness. Client identity verification and other procedures to manage fraud risks were to be included in mandatory Compulsory Professional Development training.

New South Wales introduced fraud prevention guidelines for real estate agents in 2013, providing for:

- commonsense practices and procedures for agents to confirm the identity of vendors or their representatives
- a list of possible fraud warning signs
- instructions on what agents must do if they suspect fraudulent activity
- a proof of identity checklist

The guidelines recommend that real estate agents, when confirming the identity of the owner, should do the following:

- check that the name on the agency agreement is the same as the property certificate
- conduct the check face-to-face and sight original documents to verify identity
- verify identity from an original primary photographic identification document and an original or certified copy of a secondary non-photographic identification document
- verify legal ownership of the property from an original or certified copy of a primary ownership document

An identity checklist is provided with the guidelines.

In Queensland, section 235 of the *Property Occupations Act 2014* provides that a regulation may provide for conduct standards for auctioneers, real estate agents or real estate salespersons and resident letting agents. Part 5 of the *Property Occupations Regulation 2014* contains the conduct standards for licensees and real estate salespersons. Section 19 of Part 5 requires auctioneers and real estate agents or real estate salespersons to take ‘reasonable steps’ to find out or verify the ownership of the property and property description prior to auctioning or listing a property for sale, lease or exchange. However, ‘reasonable steps’ is not defined in the regulation.

A Queensland government website, authored by the Office of Fair Trading (OFT) informs property agents of the ‘reasonable steps’ requirement and recommends agents take the following steps to check a client’s identity:

- conduct a 100-point identity check using multiple points of identification
- keep a register of all clients’ original signatures and always check that a client’s signature is a match to the signature on file
- keep records of any strange, unique or particular discussions that are had with a client
- always try to complete a property sale in person (if possible)

The OFT considers this website is a form of guidance to the industry.
The rise of identity crime in real estate featured in the May 2013 edition of the OFT Smart Business Bulletin. The Bulletin noted recent examples of sales completed without the knowledge or consent of lawful owners, and listed warning signs that might give an indication of possible fraud. The Bulletin states that ‘these recent events highlight the importance of thorough identity checks to avoid such events from occurring in the future.’

The OFT supports consideration of the ‘potential benefits of developing and publishing further resources (such as best practice guidelines) to assist property agents discharge their obligations regarding property ownership verification’, with such material likely to ‘substantially benefit from consultation with peak industry bodies such as the Real Estate Institute of Queensland and the Queensland Law Society.’

The OFT expressed some hesitation about the idea of legislatively prescribed guidelines, given subordinate legislation generally imposes mandatory obligations. Although prescribing particular steps could increase certainty regarding the operation of the legislation, it would simultaneously be likely to reduce flexibility and discretion for agents to determine the appropriate level of verification of property ownership in particular cases. Given the modern nature of property transactions often involves buyers and sellers who are based at significant distances from the physical location of the property and agent brokering the transaction, some flexibility is necessary.

Ultimately, the OFT supports visual verification of identity as part of the best practice approach and agrees it should be promoted in information and education materials. However, the OFT also considers that any requirements regarding verification of property ownership need to be sufficiently flexible to accommodate the fact that property owners may not reside interstate or overseas, or within Queensland but at some distance from the property in question.

Recommendation

5.1 The Commission recommends that the Office of Fair Trading develop and publish ‘best practice guidelines’ for property agents, including the visual verification of identity.

Verification of identity - Land transactions in Queensland

Under the Land Title Act 1994, a mortgagee and mortgage transferee must take reasonable steps to verify the identity of a mortgagor. ‘Reasonable steps’ are deemed to have been taken if the mortgagee complies with practices in the Land Title Practice Manual. Those practices do not require face-to-face verification of identity. Essentially the practices reflect the ‘100 points of identification’ provisions under Commonwealth legislation governing certain financial transactions.

The ‘100 points of identification’ practice has been preferred in Queensland, well ahead of many other states which had no Verification of Identity (VOI) practice. However, there remains potential for abuse in the absence of a visual identification check. Western Australia, South Australia and the national participation rules for e-conveyancing, as adopted by Queensland, all recommend a visual VOI check of the mortgagor. Additionally, the Queensland regime has no separate identity standard for documents executed in a foreign country.

The Land Title Act does provide that any person who witnesses an instrument executed by an individual must take reasonable steps to ensure the individual is a person entitled to sign the instrument, and the instrument must be executed in the presence of the person.

A review is currently planned of the relevant Land Title Practice Manual paragraphs (1-2495 and 2-2005) governing verification of identity of mortgagors. The Registrar of Titles informed the Commission that the aim of the review is to more closely align practices with the VOI Standard in Schedule 8 of the Queensland Participation Rules for e-conveyancing. The Registrar stated:
It is anticipated that a face to face interview will therefore be included as a requirement for a mortgagee or mortgage transferee to be deemed to have taken reasonable steps...

There is no timeframe set for the review. Consultation with other stakeholders will be undertaken prior to introducing any changes. The Commission supports that review and the inclusion of visual verification requirements in the Land Title Practice Manual.

National electronic conveyancing

Without detailing the regulatory regime for national e-conveyancing, it is sufficient to highlight that face-to-face regimes have been adopted under the Electronic Conveyancing National Law (Queensland). The Queensland Participation Rules (Version 2) (‘QPR’) require a subscriber (financial institutions and solicitors who conduct e-conveyances) to take ‘reasonable steps’ to verify the identity of prescribed persons. Compliance with the VOI Standard in Schedule 8 QPR is considered ‘reasonable steps’.

Schedule 8 includes verification of identity during a face-to-face, in-person interview between the ‘subscriber’ or the ‘subscriber agent’ and the ‘person being identified’.

Photographic identification must be provided. Where that cannot be done, the person can obtain an identity declaration in addition to other non-photographic identification documents. In such a case, the subscriber must then meet face-to-face with both the Identity Declarant and Person Being Identified.

Land transactions in Western Australia

The Western Australian VOI practice, incorporating visual identification, commenced on 1 July 2012 for all licensed settlement agents and/or mortgagees involved in a land conveyance. The practice is under current review to better align it with e-conveyancing participation rules, but the purpose of the practice is to reduce the opportunity for land title fraud committed through identity theft or other improper dealings.

Any lawyer, licensed settlement agent, or mortgagee involved in a land conveyance must be satisfied, by taking ‘reasonable steps in the circumstances’, that the person is who they claim to be and has the authority to transact with the interest in land. The two base requirements that would support ‘reasonable steps’ being taken are:

1. Identity document production – production of current, original identity documents from the categories in the VOI practice.
2. Visual verification of identity – a visual ‘face-to-face’ comparing the photograph on the current original identity documents with the person being identified.

The conveyancer, lawyer or mortgagee must confirm the identity by providing an original statement, either as a statutory declaration (on letterhead and lodged with the relevant title document) or on a transfer of land form and mortgage form incorporating the VOI statement.

Photographic identity documents must be produced to the certifier, thus reducing the reliance upon documents that are easily obtained or issued, such as utility bills.

Thus, it is likely that the requirement for both photographic identity documents and a face-to-face check produce a more robust VOI practice.

Although the VOI practice sets the standard for ‘reasonable steps’, ‘mere mechanical compliance is not sufficient’, meaning any anomalies should be considered and followed up. The practice is designed to assist those in the industry to discharge their responsibilities. It does not restrict the discretion of the Commissioner or the Registrar to register documents.

Self-represented parties are required to complete a Land Title Identity Verification Form and take it to a Landgate Identifier at a participating Australia Post office, with their photographic identification. Verification of documents outside of Australia must be undertaken by an Australian Consular Officer, who must also witness the execution of the document.
Recommendation

5.2 The Commission recommends that the Queensland Government ensure that the Land Title Practice Manual includes a requirement for visual verification of identity before a mortgagee or mortgage transferee is deemed to have taken ‘reasonable steps’ under sections 11A and 11B of the Land Title Act 1994.

IT professionals and technical security experts

People with expertise in information and communication technology and in the area of technical security are integral to the success of any type of financial crime that relies on technology. In this day and age, that means almost all organised financial crime.

Earlier in this report, it was noted that many IT professionals and technical security experts have honed their skills without gaining any tertiary or other qualifications, and that there are no regulatory requirements for practice in the information and communication technology field.

Below are some examples of the ways in which IT and technical security experts enable organised crime:

- by developing websites for use in cold-call investment frauds (also known as ‘boiler-rooms’—see below)
- by developing malware and ransomware
- by developing skimming machines
- by hacking devices to steal data

Organised crime groups are developing and recruiting their own technical experts in order to exploit the myriad of opportunities available in the cyber environment. Since the industry is global and unregulated, and skills can be easily developed by the technically adept, the only answer is for law enforcement and intelligence agencies to keep abreast of trends and advancements. It is also critical that law enforcement agencies have sufficient—and sufficiently skilled—technical personnel to identify and investigate cyber and technology-enabled crimes, including financial crimes.

Specific crime types

Financial data theft

No information was received by the Commission to suggest that professional facilitators are involved in the types of financial crime identified in the previous section, other than where it relates to money laundering. For example, remitters essentially enable the laundering of funds obtained fraudulently from transnational advance-fee frauds and skimming cases, by transferring those funds to overseas accounts. For further discussion of money laundering, see the following chapter.

Given that remitters are required to report certain transactions to AUSTRAC, the following case study, taken from AUSTRAC’s Typologies and case studies report 2014 demonstrates how remitters are used by organised crime.
Case study

AUSTRAC and investigation of advance-fee fraud

An Australian victim sent approximately $2 million to a ‘highly organised international crime syndicate committing ‘advance fee’ fraud’. AUSTRAC analysis of international funds transfer instruction (IFTI) reports showed that over seven years, the victim sent $1.2 million to overseas beneficiaries, via various remittance services and banks. There were also several suspicious matter reports (SMRs) in the AUSTRAC database, which showed that the victim used cash to fund outgoing IFTIs to multiple beneficiaries for amounts ranging between $700 and $8,500, and that the funds were transferred via remittance services. Authorities analysed AUSTRAC financial intelligence, and identified that the individual was a likely victim of fraud. The victim confirmed that he had communicated with the fraudsters over the Internet, and believed that once he paid the funds (for various fees and taxes), GBP32 million of lost funds from the United Kingdom would be released to him.51

Cold-call investment fraud

Information provided to the Commission suggests that professionals are facilitating the commission of cold-call investment fraud or ‘boiler-room’ offences. It is not known how many—if any—are willingly facilitating crime. The successful operation of a boiler-room relies heavily on professional facilitators to assist in setting up the business, presenting the business as a legitimate operation, and the day-to-day running of the business. Lawyers and accountants are said to perform enabling tasks, including ‘advising on the operation of fraudulent, high-yield investment schemes by organised crime groups and/or referring clients into such schemes’.52 Again, money laundering is an issue, particularly where the criminal organisation attached to the boiler-room is transnational.

Some of the services provided to boiler-rooms are described in the sections of this chapter below.

Accountants and financial advisors

Accountants can be engaged, willingly or unwittingly, to assist in setting up a business structure, and have been known to provide their premises as a principal place of business or registered office. Accountants could be involved in preparing financial documents for lending.

Financial advisors may also be involved in facilitating boiler-room scams, in a way similar to accountants. Of concern, the ACC describes recent instances where organised crime entities have sought to obtain Australian Financial Services licences in order to give an appearance of legitimacy to an illegal undertaking, rather than simply promoting the fraudulent investment schemes without holding a licence.53

Solicitors

According to a QPS intelligence assessment on boiler-rooms, solicitors could be engaged to draft caveats and contracts relevant to the business.54

This is demonstrated in the case of R v Henderson55 discussed above, where a solicitor prepared a business sale contract between Sports International and a person named Peter Armitage. The defendant/appellant ‘was actively involved in purporting to divest Sports International’s connection with the investment scheme to Armitage … [the] sale arrangement appears to have been calculated at distancing SIIC from investor suspicion’.56

Although there was no evidence that the solicitor had knowledge of the fraudulent nature of the scheme (as advised by QPS),57 this example highlights how solicitors may unwittingly facilitate the perpetration of boiler-room scams.
IT professionals

To give the air of authenticity to company/companies set up for the boiler-room scam, perpetrators may use the services of IT professionals for their skills in web design and development. Further, in cases where software is sent to the consumer, IT professionals may be engaged to develop that software—including multi-platform software and applications.58

Once the scam is established, it is likely that further IT support is needed. For example, crime syndicates operating boiler-room frauds have been known to engage in online ‘reputation management’. That requires expertise to remove online complaints.

Reputation management might also involve creating online material to give the false perception of legitimacy and success. Some complainants in the Carlisle and Crouch scheme, detailed in the case study in the section on investment and financial market fraud, above, were given a username and password in order to monitor their investments through a company website. The website and information accessed by each complainant was bogus, and set up by the syndicate to trick investors into thinking that the scheme was legitimate and successful.

Telephone communications systems/services

By its very name (‘cold-call’ investment fraud), a working call centre is crucial to the success of a boiler-room. Thus, premises from which to conduct the business, and a telephone system (such as PABX – Private Automated Branch Exchange) is required. Telecommunication service providers can unwittingly facilitate the commission of these offences. Many boiler-rooms use VOIP (Voice Over Internet Protocol) to prevent identification.59

A news article on the Carlisle and Crouch syndicate describes a complainant’s shock when the account into which he had poured his life savings went down, along with ‘the company’s VOIP phone line’.60

Printers

Many victims of boiler-room scams received ‘glossy brochures’ in the introductory phase which, in tandem with an ASIC company registration and a seemingly authentic website, may persuade a victim to invest. A victim of the Carlisle and Crouch scam stated to media that he found the glossy prospectus ‘quite convincing’ after initially being wary.61 Hard-copy marketing material could be prepared by graphic designers, and published by printing companies.

Examples of marketing material and screen shots of websites used by criminal cold-call investment frauds were seen by the Commission. They are professional-looking and understandably attractive to vulnerable investors.

Detective Superintendent Brian Hay told the Commission that he had spoken with the ‘president of the printing industry on the Gold Coast’ about the glossy brochures used by boiler-rooms. Detective Superintendent Hay was told that some of the industry’s members had been ‘ripped off by them not paying bills’ after the printing service was provided. One important aspect of the disruption of boiler-rooms would, therefore, involve working with this industry to have printing businesses contact police the next time an order comes in for a print run on brochures advertising certain investments known to be offered by cold-call investment scammers (for example, sports arbitrage).62

Targeting the facilitators—professional and otherwise—by engaging them in the solution is part of the QPS strategy to tackle the problem of boiler-rooms on the Gold Coast. Those strategies are dealt with in greater detail in the later section titled Responses.
(Endnotes)


38 Section 11A(3) and 11B(2) Land Title Act 1994 (Qld).


40 Section 162 Land Titles Act 1994 (Qld).

41 Statutory declaration of Elizabeth Dann, Department of Natural Resources and Mines, 8 October 2015, para 10.

42 Statutory declaration of Elizabeth Dann, Department of Natural Resources and Mines, 8 October 2015, para 11.

43 Statutory declaration of Elizabeth Dann, Department of Natural Resources and Mines, 8 October 2015, para 12.


5.5 Legislation

5.5.1 Framework

The Criminal Code (Qld) includes a number of offences dealing with dishonesty and computer-related criminal conduct. Those offences cover conduct that is susceptible to a broad range of penalties, from a maximum of two years imprisonment to life imprisonment.

<table>
<thead>
<tr>
<th>Section</th>
<th>Offence</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>391 &amp; 398</td>
<td>Stealing</td>
<td>5 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>• As a servant</td>
<td>10 years</td>
</tr>
<tr>
<td></td>
<td>• By director or office holders</td>
<td>10 years</td>
</tr>
<tr>
<td></td>
<td>• Over $5,000 in value</td>
<td>10 years</td>
</tr>
<tr>
<td>408C</td>
<td>Fraud</td>
<td>5 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>• As a director where the victim is the corporation</td>
<td>12 years</td>
</tr>
<tr>
<td></td>
<td>• Over $30,000</td>
<td>12 years</td>
</tr>
<tr>
<td>Section</td>
<td>Offence</td>
<td>Maximum Penalty</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>408D</td>
<td>Obtaining or dealing with identification information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Obtained, or deals with, for the purpose of committing or facilitating an indictable offence</td>
<td>3 years imprisonment (a misdemeanour)</td>
</tr>
<tr>
<td></td>
<td>• If the person obtaining or dealing with the identification information supplies it to a participant of a criminal organisation</td>
<td>7 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>• If a person possesses equipment for the purpose of committing or facilitating the commission of an offence of obtaining/dealing with identification information</td>
<td>3 years imprisonment (a misdemeanour)</td>
</tr>
<tr>
<td>408E</td>
<td>Computer hacking and misuse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit</td>
<td>2 years imprisonment 5 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>• If the person causes a detriment or damage or obtains a benefit for any person to the value of more than $5,000, or intends to commit an indictable offence</td>
<td>10 years imprisonment</td>
</tr>
<tr>
<td>415</td>
<td>Extortion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If carrying out the threat causes, or would be likely to cause serious personal injury</td>
<td>14 years imprisonment Life imprisonment</td>
</tr>
<tr>
<td></td>
<td>• If carrying out the threat causes, or would be likely to cause, substantial economic loss in an industrial or commercial activity conducted by a person or entity other than the offender</td>
<td>Life imprisonment</td>
</tr>
<tr>
<td>427A</td>
<td>Obtaining property by passing valueless cheques</td>
<td>2 years imprisonment (a misdemeanour)</td>
</tr>
<tr>
<td>430</td>
<td>Fraudulent falsification of records</td>
<td>10 years imprisonment</td>
</tr>
<tr>
<td>431</td>
<td>False accounting by a public officer</td>
<td>2 years imprisonment (a misdemeanour)</td>
</tr>
<tr>
<td>433</td>
<td>Receiving tainted property, including circumstances of aggravation, for example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The property was obtained by an act constituting a crime</td>
<td>7 years imprisonment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14 years imprisonment</td>
</tr>
<tr>
<td>Section</td>
<td>Offence</td>
<td>Maximum Penalty</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-----------------</td>
</tr>
<tr>
<td>442A – 442M</td>
<td>Secret commissions</td>
<td>7 years imprisonment for an individual, 3400 penalty units for a corporation, May be ordered to repay ‘valuable consideration’</td>
</tr>
<tr>
<td>488</td>
<td>Forgery and uttering</td>
<td>3 years imprisonment, 14 years imprisonment, 7 years imprisonment</td>
</tr>
</tbody>
</table>

State and Commonwealth legislation contains money-laundering offences in the Criminal Proceeds Confiscation Act 2002 (Qld) and Commonwealth Criminal Code, respectively. Reporting obligations for entities, designed to prevent money-laundering and assist in detection, are prescribed by the Financial Transactions Reporting Act 1988 (Cth) and the Anti-Money Laundering/Counter Terrorism Financing Act 2006 (Cth) (AML/CTF Act).

Money laundering is addressed in the following chapter; however, for the sake of a fulsome overview of the legislative framework for dealing with financial crime, the offence provisions of the Criminal Proceeds Confiscation Act are set out below:

Section 250 (Money-laundering)

1. A person who engages in money-laundering commits a crime. Maximum penalty—
   a. for knowingly engaging in money-laundering—3000 penalty units or 20 years imprisonment; or
   b. for recklessly engaging in money-laundering—1500 penalty units or 10 years imprisonment.

2. A person engages in money-laundering if the person knowingly or recklessly—
   a. engages, directly or indirectly, in a transaction involving money or other property that is tainted property;
   b. receives, possesses, disposes of or brings into Queensland money or other property that is tainted property; or
   c. conceals or disguises the source, existence, nature, location, ownership or control of tainted property.

Section 251 of the Act provides that the Attorney-General’s written consent must be obtained either before a proceeding starts by complaint under the Justices Act 1886, or before the proceeding progresses to hearing and decision (if the proceeding did not start by complaint). A recommendation to remove that requirement is made below.

Criminal Code Act 1995 (Cth)

Money-laundering offences are contained in sections 400.3–400.9 of the Criminal Code (Cth), with each section relating to money or property worth a specified amount or more. The higher the value of the proceeds of crime, the greater the maximum penalty. Sections 400.3 to 400.8 specify three levels of
criminality (also reflected in the maximum penalties), according to the offender’s knowledge about the money or property. Thus, the maximum penalty is higher for an offender who believes—as opposed to one who is reckless or negligent as to the fact—that the money or property is proceeds of crime.

The following table (duplicated in the chapter on money laundering) summarises those provisions and the maximum penalties:

<table>
<thead>
<tr>
<th>Section</th>
<th>Dealing in proceeds of crime – money or property worth</th>
<th>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</th>
<th>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</th>
<th>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>400.3</td>
<td>Dealing in proceeds of crime – money or property worth $1,000,000 or more</td>
<td>Maximum penalty: 25 years imprisonment or 1,500 penalty units, or both</td>
<td>Maximum penalty: 12 years imprisonment or 720 penalty units, or both</td>
<td>Maximum penalty: 5 years imprisonment or 300 penalty units, or both</td>
</tr>
<tr>
<td>400.4</td>
<td>Dealing in proceeds of crime – money or property worth $100,000 or more</td>
<td>Maximum penalty: 20 years imprisonment or 1,200 penalty units, or both</td>
<td>Maximum penalty: 10 years imprisonment or 600 penalty units, or both</td>
<td>Maximum penalty: 4 years imprisonment or 240 penalty units, or both</td>
</tr>
<tr>
<td>400.5</td>
<td>Dealing in proceeds of crime – money or property worth $50,000 or more</td>
<td>Maximum penalty: 15 years imprisonment or 900 penalty units, or both</td>
<td>Maximum penalty: 7 years imprisonment or 420 penalty units, or both</td>
<td>Maximum penalty: 3 years imprisonment or 180 penalty units, or both</td>
</tr>
<tr>
<td>400.6</td>
<td>Dealing in proceeds of crime – money or property worth $10,000 or more</td>
<td>Maximum penalty: 10 years imprisonment or 600 penalty units, or both</td>
<td>Maximum penalty: 5 years imprisonment or 300 penalty units, or both</td>
<td>Maximum penalty: 2 years imprisonment or 120 penalty units, or both</td>
</tr>
<tr>
<td>400.7</td>
<td>Dealing in proceeds of crime – money or property worth $1,000 or more</td>
<td>Maximum penalty: 5 years imprisonment or 300 penalty units, or both</td>
<td>Maximum penalty: 2 years imprisonment or 120 penalty units, or both</td>
<td>Maximum penalty: 12 months imprisonment or 60 penalty units, or both</td>
</tr>
<tr>
<td>400.8</td>
<td>Dealing in proceeds of crime – money or property of any value</td>
<td>Maximum penalty: 12 months imprisonment or 60 penalty units, or both</td>
<td>Maximum penalty: 6 months imprisonment or 30 penalty units, or both</td>
<td>Maximum penalty: 10 penalty units</td>
</tr>
</tbody>
</table>
Section 400.9 creates an offence of ‘dealing with property reasonably suspected of being proceeds of crime’. A person will be taken to have reasonably suspected money or property to be proceeds of crime if, for example, the person has engaged in conduct which involves a number of transactions structured to avoid reporting obligations under the Financial Transaction Reports Act or the AML/CTF Act.

5.5.2 Adequacy of provisions and penalties

The offence of fraud in section 408C of the Criminal Code (Qld) is the charge most commonly preferred where investment and financial market fraud (including cold-call investment frauds) is concerned.

Financial data theft, identity theft and the range of scams referred to earlier in this chapter often involve fraudulent conduct, but those crimes might also involve conduct such as obtaining or dealing with identification information or computer hacking or misuse—for example by the use of malware or ransomware to effect a fraud or extortion.

Section 408D of the Criminal Code creates the offence of obtaining or dealing with identification information, while section 408E proscribes computer hacking or misuse.

The Commission recommends below that maximum penalties be increased and/or circumstances of aggravation inserted in respect of sections 408C and 408D of the Criminal Code. Those recommendations are based, in part, on the increasing prevalence and seriousness of some types of offending (such as cold-call investment frauds) and evolving threats (particularly identity crime) that might not be adequately deterred by present penalties.

Fraud: section 408C of the Criminal Code

Section 408C is reproduced in full below. The offence covers a broad range of conduct and includes circumstances of aggravation that elevate the maximum penalty from five to 12 years imprisonment.

Section 408C - Fraud

1. A person who dishonestly –
   (a) applies to his or her own use or to the use of any person—
       (i) property belonging to another, or
       (ii) property belonging to the person, or which is in the person’s possession, either
           solely or jointly with another person, subject to a trust, direction or condition or on
           account of any other person, or
   (b) obtains property from any person; or
   (c) induces any person to deliver property to any person; or
   (d) gains a benefit or advantage, pecuniary or otherwise, to any person; or
   (e) causes a detriment, pecuniary or otherwise, to any person; or
   (f) induces any person to do any act which the person is lawfully entitled to abstain from
       doing; or
   (g) induces any person to abstain from doing any act which that person is lawfully entitled
       to do; or
   (h) makes off, knowing that payment on the spot is required or expected for any property
       lawfully supplied or returned or for any service lawfully provided, without having paid
       and with intent to avoid payment; commits the crime of fraud.’

2. An offender guilty of the crime of fraud is liable to imprisonment for 5 years save in any of
   the following cases when the offender is liable to imprisonment for 12 years, that is to say
(a) if the offender is a director of member of the governing body of a corporation, and the victim is the corporation;

(b) if the offender is an employee of another person, and the victim is the other person;

(c) if any property in relation to which the offence is committed came into the possession or control of the offender subject to a trust, direction or condition that it should be applied to any purpose or be paid to any person specified in the terms of trust, direction or condition or came into the offender’s possession on account of any other person;

(d) if the property, or the yield to the offender from the dishonesty, or the detriment caused, is of a value of $30,000 or more.

(3) For the purposes of this section –

(a) property includes credit, service, any benefit or advantage, anything evidencing a right to incur a debt or to recover or receive a benefit, and releases of obligations; and

(b) a person’s act or omission in relation to property may be dishonest even though –

(i) he or she is willing to pay for the property; or

(ii) he or she intends to afterwards restore the property or to make restitution for the property or to afterwards fulfil his or her obligations or to make good any detriment; or

(iii) an owner or other person consents to doing any act or to making any omission; or

(iv) a mistake is made by another person; and

(c) a person’s act or omission in relation to property is not taken to be dishonest, if when the person does the act or makes the omission, he or she does not know to whom the property belongs and believes on reasonable grounds that the owner can not be discovered by taking reasonable steps, unless the property came into his or her possession or control as trustee or personal representative; and

(d) person’s to whom property belongs include the owner, any joint or part owner or owner in common, any person having a legal or equitable interest in or claim to the property and any person who, immediately before the offender’s application of the property had control of it; and

(e) obtain includes to get, gain receive or acquire in any way; and

(f) if a person obtains property from any person or induces any person to deliver property to any person it is immaterial in either case whether the owner passes or intends to pass ownership in the property or whether he or she intends to pass ownership in the property to any person.

It is also noteworthy that section 568(3) of the Criminal Code allows multiple charges of fraud to be ‘bundled up’ into one charge. That subsection provides:

In an Indictment against a person for fraud the person may be charged and proceeded against on 1 charge even though –

(a) any number of specific frauds of the same type has been committed, whether or not each specific act of fraud can be identified; or

(b) the frauds have extended over any space of time; or

(c) property applied belongs to different persons, and has come into the possession or control of the accused person at different times and subject to different trusts, directions, conditions, or duties to account; or
(d) the property, benefit, detriment or inducement belongs to or is caused to different persons.’

Therefore, in a case where multiple frauds have been committed, each of them yielding less than $30,000—but overall amounting to more—an offender can be indicted on one count of fraud with a circumstance of aggravation (that the yield was more than $30,000), thereby increasing liability from five to 12 years imprisonment. That approach was taken in R v Carlisle and Crouch1 (Case study above) where the indictment charged each offender with one count of fraud, involving multiple frauds on multiple victims. Both offenders were sentenced to 10 years imprisonment.

The concern of the Commission is that in a case worse than Carlisle and Crouch, where only one charge of fraud is preferred, the heaviest penalty available to a sentencing Court is 12 years imprisonment. That is less than the 14-year maximum penalty available in some cases of forgery and uttering and receiving tainted property.

The Commission considers that this is an anomaly that should be resolved by increasing the maximum penalty for fraud, involving existing circumstances of aggravation under section 408C(2) of the Criminal Code, from 12 to 14 years imprisonment. Two additional circumstances of aggravation, which would carry a maximum penalty of 20 years imprisonment, are also recommended following the analysis below.

The Commission undertook a comparative analysis of fraud and related offences in other Australian jurisdictions in considering the adequacy of the framework provided by the Queensland Criminal Code—in particular section 408C—to deal with the broad range of fraudulent conduct, including cyber and technology-enabled fraud. Relevantly, the Terms of Reference required the Commission to consider the adequacy of current legislation ‘to prevent and effectively investigate and prosecute organised criminal activity.’2

The table below sets out a range of interstate and Commonwealth offences considered:

<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATION</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>New South Wales</td>
<td>Division 1, Part 4AA Fraud of the Crimes Act 1900 provides definitions of ‘Deception’, ‘Obtaining property belonging to another’ and ‘Obtaining financial advantage or causing financial disadvantage’.</td>
<td>10 years imprisonment</td>
</tr>
</tbody>
</table>

Offences are listed in Division 2 of the same Part:

192E Fraud

(1) A person who, by any deception, dishonestly:
   (a) obtains property belonging to another, or
   (b) obtains any financial advantage or causes any financial disadvantage,
   is guilty of the offence of fraud.

192F Intention to defraud by destroying or concealing accounting records

(1) A person who dishonestly destroys or conceals any accounting record with the intention of:
   (a) obtaining property belonging to another, or
   (b) obtaining a financial advantage or causing a financial disadvantage,
   is guilty of an offence.
<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATION</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queensland</td>
<td>192G Intention to defraud by false or misleading statement</td>
<td>5 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>A person who dishonestly makes or publishes, or concurs in making or publishing, any statement (whether or not in writing) that is false or misleading in a material particular with the intention of:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) obtaining property belonging to another, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) obtaining a financial advantage or causing a financial disadvantage,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is guilty of an offence.</td>
<td></td>
</tr>
<tr>
<td>Queensland</td>
<td>192H Intention to deceive members or creditors by false or misleading statement of officer of organisation</td>
<td>7 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>(1) an officer of an organisation who, with the intention of deceiving members or creditors of the organisation about its affairs, dishonestly makes or publishes, or concurs in making or publishing, a statement (whether or not in writing) that to his or her knowledge is or may be false or misleading in a material particular is guilty of an offence.</td>
<td></td>
</tr>
<tr>
<td>Victoria</td>
<td>The Crimes Act 1958 provides the following relevant offences, under the heading ‘Fraud and blackmail’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>81 Obtaining property by deception</td>
<td>10 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, is guilty of an indictable offence and liable to level 5 imprisonment (10 years maximum).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This section then defines terms including ‘deception’ and ‘obtains property’.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>82 Obtaining financial advantage by deception</td>
<td>10 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>(1) A person who by any deception dishonestly obtains for himself or another any financial advantage is guilty of an indictable offence and liable to level 5 imprisonment (10 years maximum).</td>
<td></td>
</tr>
</tbody>
</table>
191 Fraudulently inducing persons to invest money

(1) Any person who, by any statement, promise or forecast which he knows to be misleading false or deceptive or by any dishonest concealment of material facts or by the reckless making of any statement promise or forecast which is misleading false or deceptive, induces or attempts to induce another person—

(a) to enter into or offer to enter into—

(i) any agreement for or with a view to acquiring, disposing of subscribing in or underwriting securities or lending or depositing money to or with any corporation; or

(ii) any agreement the purpose or pretended purpose of which is to secure a profit to any of the parties from the yield of securities or by reference to fluctuations in the value of securities; or

(b) to acquire or offer to acquire any right or interest under any arrangement the purpose or effect or pretended purpose or effect of which is to provide facilities for the participation by persons in profits or income alleged to arise or to be likely to arise from the acquisition holding management or disposal of any property other than securities; or

(c) to enter into or offer to enter into an agreement the purpose or pretended purpose of which is to secure a profit to any of the parties by reference to fluctuations in the value of any property other than securities—

shall be guilty of an indictable offence and liable to level 4 imprisonment (15 years maximum).

(2) Any person guilty of conspiracy to commit any offence against the last preceding subsection shall be punishable as if he had committed such an offence.
<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATION</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Australia</td>
<td>Part 5 of the <em>Criminal Law Consolidation Act 1935</em> contains ‘Offences of dishonesty’. Section 130 provides Interpretation of the terms used throughout the Part and section 131 defines ‘dishonesty’.</td>
<td>10 years imprisonment - ‘basic’ offence; 15 years - ‘aggravated’ offence</td>
</tr>
</tbody>
</table>

### 139—Deception

A person who deceives another and, by doing so—
(a) dishonestly benefits him/herself or a third person; or
(b) dishonestly causes a detriment to the person subjected to the deception or a third person, is guilty of an offence.

### 141—Dishonest manipulation of machines

(1) A person who dishonestly manipulates a machine in order to—
(a) benefit him/herself or another; or
(b) cause a detriment to another,
is guilty of an offence. ...

(2) A person who dishonestly takes advantage of the malfunction of a machine in order to—
(a) benefit him/herself or another; or
(b) cause a detriment to another,
is guilty of an offence.

‘Aggravated offences’ are those committed in one or more of the circumstances listed in section 5AA *Criminal Law Consolidation Act 1935* (SA)

<table>
<thead>
<tr>
<th>Western Australia</th>
<th>The Criminal Code (WA)</th>
<th></th>
</tr>
</thead>
</table>

### 409. Fraud

(1) Any person who, with intent to defraud, by deceit or any fraudulent means –
(a) obtains property from any person; or
(b) induces any person to deliver property to another person; or
(c) gains a benefit, pecuniary or otherwise, for any person; or
(d) causes a detriment, pecuniary or otherwise, to any person; or

If the person deceived is over 60 years of age – 10 years imprisonment;
In any other case – 7 years imprisonment.
Other maximum penalties are provided upon summary conviction.
<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATION</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(e) induces any person to do any act that the person is lawfully entitled to abstain from doing; or (f) induces any person to abstain from doing any act that the person is lawfully entitled to do, is guilty of a crime and is liable ...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fraud cannot be dealt with summarily where the value of the relevant benefit/detriment is over $10,000.</td>
</tr>
<tr>
<td>Tasmania</td>
<td>The Criminal Code (Tas)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>252A. Acquiring a financial advantage</td>
<td>Section 389 provides that unless expressly stated otherwise, the maximum penalty for all offences is either 21 years imprisonment or a fine, or both.</td>
</tr>
<tr>
<td></td>
<td>(1) Any person who by any deception dishonestly acquires for himself or for any other person any financial advantage is guilty of a crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>253A. Fraud</td>
<td>The Sentencing Act 1997 provides sentencing options.</td>
</tr>
<tr>
<td></td>
<td>Any person who, with intent to defraud, or by deceit or any fraudulent means – (a) obtains property from a person; or (b) induces a person to – (i) deliver, transfer, or assign, property to another person; or (ii) cause property to be delivered, transferred, or assigned, to another person; or (c) gains a benefit, pecuniary or otherwise, for any person; or (d) causes a detriment, pecuniary or otherwise, to any person; or (e) induces any person to do an act that the person is lawfully entitled to abstain from doing; or (f) induces any person to abstain from doing any act that the person is lawfully entitled to do – is guilty of a crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer-related fraud is also an offence, under Chapter XXVIIA – Crimes Relating to Computers:</td>
<td></td>
</tr>
</tbody>
</table>
257B. Computer-related fraud

A person who, with intent to defraud –

(a) destroys, damages, erases, alters or otherwise manipulates data stored in, or used in connection with, a computer; or

(b) introduces into, or records or stores in, a computer or system of computers by any means data for the purpose of –

(i) destroying, damaging, erasing or altering other data stored in that computer or that system of computers; or

(ii) interfering with, interrupting or obstructing the lawful use of that computer or that system of computers or the data stored in that computer or system of computers; or

(c) otherwise uses a computer –

is guilty of a crime.

Commonwealth

The Commonwealth Criminal Code also contains offences akin to fraud, where there is some connection with the Commonwealth (in other words, the property belongs to a Commonwealth entity, the complainant is a Commonwealth entity). These offences are most commonly seen in Centrelink frauds and tax evasion schemes.

134.1 Obtaining property by deception

(1) A person is guilty of an offence if:

(a) the person, by a deception, dishonestly obtains property belonging to another with the intention of permanently depriving the other of the property; and

(b) the property belongs to a Commonwealth entity.

134.2 Obtaining a financial advantage by deception

(1) A person is guilty of an offence if:

(a) the person, by a deception, dishonestly obtains a financial advantage from another person; and

(b) the other person is a Commonwealth entity.
<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATION</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>135.1 General dishonesty</strong></td>
<td>5 years imprisonment</td>
</tr>
<tr>
<td></td>
<td>(1) A person is guilty of an offence if:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) the person does anything with the intention of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dishonestly obtaining a gain from another person;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) the other person is a Commonwealth entity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3) A person is guilty of an offence if:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) the person does anything with the intention of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dishonestly causing a loss to another person; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) the other person is a Commonwealth entity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3) A person is guilty of an offence if:</td>
<td>12 months</td>
</tr>
<tr>
<td></td>
<td>(a) the person engages in conduct; and</td>
<td>imprisonment</td>
</tr>
<tr>
<td></td>
<td>(aa) as a result of that conduct, the person obtains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a financial advantage for himself or herself from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>another person; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ab) the person knows or believes that he or she is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not eligible to receive that financial advantage;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ac) the other person is a Commonwealth entity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>135.4 Conspiracy to defraud</strong></td>
<td>10 years</td>
</tr>
<tr>
<td></td>
<td>Obtaining a gain</td>
<td>imprisonment</td>
</tr>
<tr>
<td></td>
<td>(1) A person is guilty of an offence if:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) the person conspires with another person with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the intention of dishonestly obtaining a gain from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a third person; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) the third person is a Commonwealth entity.</td>
<td></td>
</tr>
</tbody>
</table>

Given the Terms of Reference and the focus on cold-call investment frauds the Commission was particularly interested in two of the above-mentioned offences: section 191 (Fraudulently inducing persons to invest money) of the *Crimes Act 1958* (Vic) and section 257B (Computer related fraud) of the *Criminal Code* (Tas).

At first blush, the Victorian provision—carrying a maximum penalty of 15 years imprisonment—might appear to fill a gap in the Queensland legislative framework. However, the Commission learned that it is not a new provision designed to deal with new problems, but rather an offence that has been a part of the *Crimes Act* since at least the 1970s. It is also rarely used. The Commission found only two decisions, neither of which demonstrated that a similar provision would be useful to combat organised crime in Queensland.

Likewise, cases involving the Tasmanian provision, dealing specifically with computer-related fraud, show that section 408C of the Queensland Criminal Code is apt to deal with the conduct attracting that charge.

While the Commission is satisfied that existing offence provisions are adequate to prosecute organised criminal activity, there is a concern that existing circumstances of aggravation and maximum penalties are insufficient to provide the necessary deterrence.
As foreshadowed above, in circumstances where it is known that offenders at the top of the hierarchy of a cold-call investments fraud are engaged in organised crime to the significant detriment of victims, the Commission considers it incongruent that the maximum penalty (12 years in the case of a circumstance of aggravation) under section 408C of the Criminal Code is less than that for forgery and uttering, or for receiving tainted property (14 years in the case of a circumstance of aggravation).

Further, a number of recent examples demonstrate that the existing maximum penalty for an aggravated fraud (over $30,000) is inadequate to deal with the most serious types of fraudulent conduct.

In *R v Morehu-Barlow*, a now-notorious public servant—who referred to himself as a ‘Tahitian prince’—committed frauds on the State amounting to more than $16 million. An effective sentence of 14 years imprisonment (two years beyond the maximum penalty for aggravated fraud) could only be achieved by imposing cumulative terms of imprisonment for different offences.

That approach was the subject of argument on appeal, with Morehu-Barlow’s counsel contending that cumulative sentences should not be imposed in order to circumvent the maximum penalty in the absence of a proper reason for doing so. Fraser JA (with whom Gotterson JA and McMeekin J agreed) held that the approach was permissible in order to ensure that the punishment imposed was proportionate to the total criminality.

The same approach was taken to achieve effective sentences of 13 years (although that was reduced to 11 years on appeal) in *R v Lovell* (case study above), and 15 years in *R v O’Carrigan*. Lovell operated a protracted ‘Ponzi’ scheme that defrauded multiple victims of a combined sum of $11.5 million. O’Carrigan was the manager and finance administrator of a construction company which he defrauded of more than $20.5 million over 12 years.

None of those examples involved the kind of organised crime that characterises cold-call investment frauds, so that it is likely that the courts will see cases calling for heavier penalties. In order to achieve that within the existing framework, courts will need to impose cumulative sentences (an approach that might later become the subject of argument on appeal).

A further, significant difficulty will be faced by a court confronted with a serious example of fraud where only one offence is charged. In that case, there is no opportunity to consider accumulating sentences. *R v Carlisle and Crouch* is a recent example, involving a cold-call investment fraud, where only one charge of fraud was preferred against each offender. Sentences of 10 years imprisonment were imposed for each offender for his involvement in managing the boiler-room which fleeced some 400 people approximately $4.6 million (see Case study above).

Cold-call investment frauds are undoubtedly a type of organised crime; however, there is no circumstance of aggravation in section 408C that adequately reflects that. Further, fraud under section 408C is not a ‘declared offence’ pursuant to the *Vicious Lawless Association Disestablishment Act 2013* (VLAD Act) and is therefore not susceptible to the mandatory sentencing regime established by it.

Given that, and in light of the difficulties that might be encountered in imposing adequate punishment (and achieving effective deterrence) in cases involving serious and organised financial crime, the Commission considered the need for new circumstances of aggravation that would carry a heavier maximum penalty.

**Application of the Vicious Lawless Association Disestablishment Act 2013**

A court sentencing a ‘vicious lawless associate’ for a ‘declared offence’ must impose a sentence of 15 years imprisonment served wholly in a corrective services facility, in addition to a sentence for the offence under the law apart from the VLAD Act.

A person is a vicious lawless associate if the person commits a ‘declared offence’, and if ‘at the time the offence is committed, or during the course of the commission of the offence, is a participant in the affairs of an association (relevant association)’, and ‘did or omitted to do the act that constitutes the declared offence for the purposes of, or in the course of participating in the affairs of, the relevant association’.
Section 4 of the VLAD Act defines a ‘declared offence’ as an offence mentioned in Schedule 1 of the Act, or an offence prescribed under a regulation to be a ‘declared offence’. Section 408C is not a provision mentioned in Schedule 1, nor is it prescribed under a regulation. Therefore, the VLAD Act has no application to persons committing fraud as part of an association of criminals where the commission of the fraud is for the purposes of, or in the course of participating in the affairs of, the association.

The State offence of money-laundering (section 250 of the Criminal Proceeds Confiscation Act) is, however, mentioned in Schedule 1, and is therefore a ‘declared offence’. As discussed earlier, consent from the Attorney-General is required in order to proceed with a money-laundering offence, regardless of whether a person is charged under the VLAD Act regime.

To date, the VLAD Act provisions have not been enlivened for any matter involving money-laundering in a fraud or fraud-related context. In fact, the Commission was told that since 1 January 2012, only four persons have had matters finalised, where a charge of money-laundering was preferred pursuant to section 250 of the Criminal Proceeds Confiscation Act. Of those four, two were finalised by pleas of guilty and two were ‘discontinued after pleas of guilty were entered to substitute charges of fraud’. None involved the application of the VLAD Act.

The Queensland Police Service (QPS) suggested that the application of the VLAD Act could be extended to include fraud under section 408C of the Criminal Code, for the following reasons:

Investigations of CCI (cold-call investment) frauds have clearly identified a syndicated approach to the formation, operation and eventual ‘phoenixing’ into another fraudulent investment or sports arbitrage entity. The ability to apply the circumstance of aggravation under the VLAD Act to fraud offences is logical and desirable given the level of sophistication and organisation that makes such offending more effective.

The VLAD Act circumstance of aggravation could be applied to the organisers, those identified as being an integral part of the fraud operation and to the nominated directors, if sufficient evidence of the criminal association was available.

As previously noted in the chapter of this report on outlaw motorcycle gangs, the VLAD Act formed part of a package of reforms that targeted outlaw motorcycle gangs by providing a crushing mandatory, cumulative sentencing regime.

As serious as boiler-room frauds can be, the Commission does not consider that the application of the VLAD Act sentencing regime is appropriate or necessary to achieve condign punishment for offenders, in accordance with the only purposes for which sentences may be imposed. Section 9 of the Penalties and Sentences Act 1992 sets out those purposes as follows:

(a) to punish the offender to an extent or in a way that is just in all the circumstances; or
(b) to provide conditions in the court’s order that the court considers will help the offender to be rehabilitated; or
(c) to deter the offender or other persons from committing the same or a similar offence; or
(d) to make it clear that the community, acting through the court, denounces the sort of conduct in which the offender was involved; or
(e) to protect the Queensland community from the offender; or
(f) a combination of 2 or more of the purposes mentioned in paragraphs (a) to (e).

The mandatory sentencing regime in the VLAD Act also, essentially, renders nugatory section 9(2) of the Penalties and Sentences Act, which provides a list of matters that a court must have regard to in sentencing an offender—including, for example:

- the maximum and minimum penalty prescribed for the offence; and
- the extent to which the offender is to blame for the offence; and
- any damage injury or loss caused by the offender; and
- the offender’s character, age and intellectual capacity.
The Commission is of the view that the purposes of sentencing serious fraud offenders, considering the matters relevant to the exercise of the sentencing discretion by a court, can be more fairly achieved by increasing the maximum penalty available for those guilty of existing aggravated fraud offences, and inserting a new circumstance of aggravation for frauds over $100,000, and for frauds committed by an offender where the fraudulent conduct involved the planned and systematic targeting of the public.

A new circumstance of aggravation for fraud

As part of the package of reforms in 2013, the Criminal Law (Criminal Organisations Disruption) Amendment Act 2013 inserted a circumstance of aggravation, relating to participants of criminal organisations, into section 408D (Obtaining or dealing with identification information), which now relevantly provides –

(1) A person who obtains or deals with another entity’s identification information for the purpose of committing, or facilitating the commission of, an indictable offence commits a misdemeanour.

Maximum penalty – 3 years imprisonment.

(1AA) If the person obtaining or dealing with the identification information supplies it to a participant in a criminal organisation [emphasis added], the person is liable to imprisonment for 7 years.

(1AB) For an offence defined in subsection (1) alleged to have been committed with the circumstance of aggravation mentioned in subsection (1AA), it is a defence to the circumstance of aggravation to prove that the criminal organisation is not an organisation that has, as 1 of its purposes, the purpose of engaging in, or conspiring to engage in, criminal activity.

No similar circumstance of aggravation, or offence particular to participants of criminal organisations, was introduced to section 408C (Fraud).

The meaning of ‘participant in a criminal organisation’ requires reference to the following series of provisions –

• Section 60A (Participants in criminal organisations being knowingly present in public places) of the Criminal Code, for the definition of ‘participant’ in a criminal organisation; and

• Section 1 (Definitions) of the Criminal Code for the definition of ‘criminal organisation’; and

• Sections 6 and 7, and Schedule 1 of the Criminal Organisation Act 2009 (Qld) for the definitions of ‘serious criminal activity’ and ‘serious criminal offence’.

In the result, fraud (under section 408C) is a ‘serious criminal activity’ to which the definition of ‘criminal organisation’ might apply. A ‘criminal organisation’ means –

(a) an organisation of 3 or more persons –

(i) who have as their purpose, or 1 of their purposes, engaging in, organising, planning, facilitating, supporting, or otherwise conspiring to engage in, serious criminal activity as defined under the Criminal Organisation Act 2009; and

(j) who, by their association, represent an unacceptable risk to the safety, welfare, or order of the community; or

(b) a criminal organisation under the Criminal Organisation Act 2009; or

(c) an entity declared under a regulation to be a criminal organisation.

Although the Commission considers the reference to a ‘participant’ is unnecessary and problematic for the reasons articulated in the chapter discussing a specific offence of organised crime, if the legislative framework continues to include the definition of ‘criminal organisation’ in the Code and associated definitions in the Criminal Organisation Act, a similarly framed circumstance of aggravation might be applied to section 408C.

Alternatively, in the event that the existing definitions become defunct after reviews of the 2013 amendments and the Criminal Organisation Act, a circumstance of aggravation that would apply where the fraudulent conduct involved the planned, systematic targeting of the public is recommended.
In any event, there should be an additional circumstance of aggravation for frauds that involve property, or yield to an offender, or detriment caused of a value of $100,000 or more. That would recognise that the existing circumstance of aggravation (for frauds of a value over $30,000) deals with a relatively modest sum by today’s standards.

### Recommendations

**The Commission recommends that:**

5.3 The Queensland Government amend section 408C (Fraud) of the Criminal Code by increasing the maximum penalty for aggravated fraud in subsection (2) to 14 years imprisonment.

5.4 The Queensland Government amend section 408C (Fraud) of the Criminal Code by inserting an additional circumstance of aggravation, to apply if the property, or the yield to the offender from the dishonesty, or the detriment caused, is of a value of $100,000 or more.

In that case, the maximum penalty would be 20 years imprisonment.

5.5 The Queensland Government amend section 408C (Fraud) of the Criminal Code by inserting an additional circumstance of aggravation, carrying a maximum penalty of 20 years imprisonment, where the fraudulent conduct involved the planned and systematic targeting of the public.

#### Obtaining or dealing with identification information: section 408D of the Criminal Code

The offence of ‘obtaining or dealing with identification information’ was originally inserted into the Criminal Code in 2007 after identity fraud had been identified as a significant threat nationally, and particularly in response to credit and debit card ‘skimming’. It is based on the model credit card skimming offence that was endorsed by the Model Criminal Code Officers Committee in its discussion paper of March 2004. Section 408D was designed to fill a gap in legislation, where a person had identification information for a criminal purpose but did not commit a substantive offence with it (or same could not be proved). It was enacted as a misdemeanour, and carries a maximum penalty of three years imprisonment.

The Explanatory Memorandum described the conduct targeted by the provision as follows:

> …here personal financial details are obtained through a variety of methods including the use of electronic devices fitted to banks’ automatic teller machines, and then used to effect financial transactions (often overseas) that result in individuals, financial institutions, insurers and ultimately the community losing significant sums of money.

The offence is not limited to ‘skimming’ offences, and in fact, does not appear to have been used for that kind of offending (where Commonwealth money-laundering charges have been preferred instead, probably because of the high maximum penalty that offence attracts).

The sentencing statistics recorded on the Queensland Sentencing Information Service for section 408D(1) offences record only 52 instances in the Magistrates Court, and five in the higher courts, between January 2011 and December 2014. Furthermore, a review of single-judge decisions reveals that offenders are often convicted of an offence under section 408D in conjunction with other, more serious offences. That accords with the original intent of the Parliament that section 408D deal with preparatory, rather than substantive offending.

Section 408D currently provides:

> (2) A person who obtains or deals with another entity’s identification information for the purpose of committing, or facilitating the commission of, an indictable offence commits a misdemeanour.

Maximum penalty – 3 years imprisonment.
If the person obtaining or dealing with the identification information supplies it to a participant in a criminal organisation, the person is liable to imprisonment for 7 years.

For an offence defined in subsection (1) alleged to have been committed with the circumstance of aggravation mentioned in subsection (1AA), it is a defence to the circumstance of aggravation to prove that the criminal organisation is not an organisation that has, as 1 of its purposes, the purpose of engaging in, or conspiring to engage in, criminal activity.

A person who possesses equipment for the purpose of committing, or facilitating the commission of, an offence against subsection (1), commits a misdemeanour.

Maximum penalty – 3 years imprisonment.

For subsection (1), it is immaterial whether the other entity if alive or dead, or exists or does not exist, or consent or does not consent to the obtaining or dealing.

When a court is sentencing a person for an offence against subsection (1), the court may order that the court’s certificate be issued to the other entity stating the offence, the entity’s name and anything else the court considers relevant for the entity’s benefit.

The order may be made on the court’s own initiative or on application by the entity or prosecutor.

If the person is sentenced on a plea of guilty, the certificate may be given to the entity immediately.

If subsection (5) does not apply, the certificate must not be given to the entity until the later of the following –

(a) the end of any period allowed for appeal against conviction;

(b) if an appeal is started – the end of any proceedings on the appeal.

In this section -

dealing, with identification information, includes supplying or using the information.

digital signature means encrypted electronic or computer data intended for the exclusive use of a particular person as a means of identifying himself or herself as the sender of an electronic communication.

identification information of another entity, means information about, or identifying particulars of, the entity that is capable of being used, whether alone or in conjunction with other information, to identify or purportedly identify the entity.

Examples for an entity that is an individual –

- information about the individual or the individual’s relatives including name, address, date of birth, marital status and similar information
- the individual’s driver licence or driver licence number
- the individual’s passport or passport number
- anything commonly used by an individual to identify himself or herself, including a digital signature
- the individual’s financial account numbers, user names and passwords
- a series of numbers or letters (or a combination of both) intended for use as a means of personal identification
- any data stored or encrypted on the individual’s credit or debit card
- biometric data relating to the individual
- the individual’s voice print
- a false driver licence or other false form of identification for a fictitious individual
Examples for an entity that is a body corporate –

- the body corporate’s name
- the body corporate’s ABN
- the body corporate’s financial account numbers
- any data stored or encrypted on a credit or debit card issued to the body corporate
- obtaining, identification information includes possessing or making the information.
- participant, in a criminal organisation, see section 60A.

Subsection (1A) was added by amendment in 2010 to provide an alternative charge to that set out in section 510 (Instruments and materials for forgery) of the Code which provides:

Any person who unlawfully –

(a) makes, or starts or prepared to make, a thing with intent to use it to forge a document; or
(b) possesses a thing with intent to use it to forge a document; or
(c) uses a thing to forge a document; or
(d) disposes of a thing that has been used to forge a document;

commits a crime.

Maximum penalty – 14 years imprisonment.

To ‘forge a document’ means make, alter, deal with the document so that the whole of it or a material part of it –

(a) purports to be what, or of an effect that, in fact it is not; or
(b) purports to be made, altered or dealt with by a person who did not make, alter or deal with it or by or for some person who does not, in fact exist; or
(c) purports to be made, altered or dealt with by authority of a person who did not give that authority; or
(d) otherwise purports to be made, altered or dealt with in circumstances in which it was not made, altered or dealt with.

A ‘document’ includes –

(a) anything on which there is writing; and
(b) anything on which there are marks, figures, symbols, codes, perforations or anything else having a meaning for a person qualified to interpret them; and
(c) a record.17

A ‘record’ means any thing or process –

(a) on or by which information is recorded or stored; or
(b) by means of which sounds, images, writings, messages or anything else having meaning can be conveyed in any way in a visible or recoverable form;

even if the use or assistance of some electronic, electrical, mechanical, chemical or other device or process is required to recover or convey the information or meaning.18

Those definitions make it clear that the reference to ‘document’ in the offence of forgery covers a much broader range of recorded information than the term ordinarily conveys. That offence, carrying a maximum of 14 years imprisonment, would apply to a person who makes credit or debit cards, drivers’ licences and other forms of identification using stolen identity data, or who has equipment (for example a skimming device) with intent to forge such ‘documents’.
The Explanatory Memorandum to the 2010 amendments states that although section 510 of the Criminal Code makes it an offence to possess instruments and materials for forgery, the application of that offence was limited and carried a maximum penalty of 14 years.\(^{19}\)

During debate on the Bill, the then-Attorney-General and Minister for Industrial Relations, the Honourable Cameron Dick MP, stated:

> It [the new subsection 408D(1A)] does not amount to a reduction of the maximum penalty. The elements of the new offence are different from the existing offence. In order to convict a person under section 510 of the Criminal Code, it is necessary to prove that the person is intending to use the thing to forge a document. Therefore, in order to gain a conviction under section 510 the prosecution must prove beyond a reasonable doubt the requisite intent which includes proof beyond reasonable doubt that the information or thing being forged is a document ... When police apprehend a person who possesses equipment, they have options to charge under existing section 510 if the evidence exists to support the charge. If not, then this new section provides an alternative charge.\(^{20}\)

The ALP Member for Barron River (then The Hon. Mr Wettenhall MP) added -

> The bill creates a new offence of possessing equipment that can be used to make identification information with intent ... The offence will fill a gap in the legislation that prevents the Queensland Police Service from prosecuting a person if they possess but have not yet used equipment that can be used to make identification information. For example, the offence could be used to prosecute a person who had possession of a miniature camera, a magnetic strip reader and a quantity of cards with blank magnetic strips and who intended to skim credit card details from an ATM. Currently, the police are constrained to wait until the person has actually skimmed those details.

> This amendment complements the existing provision contained in section 408D of the Code so that possession of equipment, which is only preparatory to the other offence provision, is also captured. Victims will appreciate that there is no need for the police to wait until an actual dealing with the information has taken place before they can charge an offender.\(^{21}\)

Section 408D(1AA) was part of the suite of offences, focused on outlaw motorcycle gangs, introduced by the former Government in 2013. While the Commission supports a circumstance of aggravation for those who unlawfully obtain or deal with identification information as part of a criminal organisation, the circumstance of aggravation in its present form applies only to the supply of such information to a ‘participant in a criminal organisation’. Again, ‘participant’ derives its meaning from section 60A of the Criminal Code, which calls for a minimum mandatory term of imprisonment when ‘participants’ associate with one another.

If the aim is to combat organised crime, rather than dealings between people deemed to be ‘participants’ but who might be operating alone or outside the ‘criminal organisation’, section 408A(1AA) would be better framed without reference to the term ‘participant’. An alternative might be found in section 5AA of the Criminal Law Consolidation Act (SA), which relevantly provides as follows:

Section 5AA

> (ga) - 
> (i) the offender committed the offence for the benefit of a criminal organisation, or 2 or more members of a criminal organisation, or at the direction of, or in association with, a criminal organisation...

Using similar terminology, section 408D(1AA) would aggravate the supply of identification information for the benefit of a criminal organisation, or 2 or more members of a criminal organisation, or at the direction of, or in association with, a criminal organisation, rather than simply to a participant in a criminal organisation.
The recommended increase in the maximum penalty is explained further below.

Recommendation

5.6 The Commission recommends that the Queensland Government further amend section 408D (Obtaining or dealing with identification information) of the Criminal Code by extending the ambit of the circumstance of aggravation in subsection (1AA) as follows:

(1AA) If the person obtaining or dealing with the identification information supplies it for the benefit of a criminal organisation, or 2 or more members of a criminal organisation, or at the direction of, or in association with, a criminal organisation, the person is liable to ....

Acting Detective Superintendent Terry Lawrence told the Commission that since the establishment of a project in November 2014 to ‘better capture, record and manage reported card skimming offences in Queensland’,22 ‘skimming’ activity is not significant:

Anecdotally, this reduction in card skimming appears to be partly the result of ‘chip and pin’ technology implemented by card issuers, and partly due to financial institutions under reporting skimming incidents.

This view on chip technology is supported by other information that the Commission received from professionals in the financial sector.

Given the downward trend in this kind of offending, and the successful prosecutions using existing provisions, the Commission does not recommend new offences. The Commission does, however, recommend increasing the maximum penalties for offending under section 408D to reflect the seriousness of identity crime, and to bring the maximum penalties into line with the penalties for fraud under section 408C.

Recommendation

5.7 The Commission recommends that the Queensland Government amend section 408D (Obtaining or dealing with identification information) of the Criminal Code to increase the maximum penalties as follows:

1. 5 years imprisonment
2. (1AA) 14 years imprisonment
3. (1A) 5 years imprisonment.

5.5.3 Regulatory Framework

Office of Fair Trading

The Queensland Office of Fair Trading has a number of powers, contained in Part 5 of the Fair Trading Act 1989 (Qld). When working in tandem with QPS, those powers can be directly utilised to disrupt and investigate cold-call investment frauds and other financial market frauds.

Section 89 allows an inspector (discharging any of the Commissioner’s functions under the Act, or for any other purpose of the Act) to enter any premises, where conduct relating to a contravention of the Act is known or reasonably suspected of being associated with a contravention. The types of premises and types
of conduct are set out in sub-sections (1)(a) – (d). Sub-section (1)(e) sets out what the inspector is entitled to do upon entry of the premises. Sub-section (1)(f) further empowers an inspector to ‘make such inquiry and examination as the inspector believes to be necessary or desirable to assist the discharge or exercise of any function or power under this Act or to ascertain whether any contravention of this Act has been, is being, or is likely to be committed.’ Prior to entry, the inspector must obtain a warrant to enter, unless the occupier has given permission (subsection 2). The inspector may retain any seized property for as long as necessary for the purposes of the act (subsection 6).

The Office of Fair Trading also has the power to obtain information (section 90):

(1) In relation to any matter relevant to the operation or enforcement of this Act, an inspector may require a person (either by oral or written requisition) to furnish-

(a) any information; and
(b) any records or a copy of them;

in the person’s possession.

This power is used to obtain bank records (see discussion below on notices to produce). A penalty applies for non-compliance with the notice, which is a maximum of 100 penalty units.

Section 91 provides that a person shall not obstruct an inspector in the exercise of powers under the Act, with a maximum penalty of 100 penalty units.

There are also powers to seize goods, contained in section 91A, where goods have been supplied in contravention of the Act. Offences are contained in section 92, and include offences against the Australian Consumer Law Act (Qld), chapter 4.

In interview with the Commission, Steven L’Barrow, Director, Tactical Compliance of the Office of Fair Trading, stated the following about boiler-room investigations and the powers of the Office of Fair Trading:

[this] type of criminal enterprise is really not our jurisdiction, and we’ll certainly help the police, and we’ve said that we’ll help them where we can with what powers that we have, but our resources are best used in trying to warn people about these types of calls.23

The Office of Fair Trading has worked collaboratively with QPS in multi-agency approaches. For example, in 2009, Office of Fair Trading Operations Marble 1 and 2 were conducted with the police and the Australian Competition and Consumer Commission, focusing on intelligence-gathering and disruption of boiler-rooms on the Gold Coast.24 The Office of Fair Trading was at the front of the investigation, due to their broad section 89 entry powers.

Those powers are to search only, which means if fraudulent conduct is occurring and employees are present but leave on Office of Fair Trading arrival, there are no powers to detain.

The Office of Fair Trading cannot take action in regards to proceeds of crime, but it can seek compensation orders against company directors and monetary penalties for directors.

In addition to those powers, the Office of Fair Trading also has a broad power to ‘publicly name a trader or warn about particular practices.’25 The power is used sparingly so as not to name a legitimate business, with all the repercussions that would arise from such naming. Consequently, only the Executive Director or the Commissioner (the Deputy Director-General) can authorise the public naming of a trader, warning consumers not to deal with that business. A recent example of that power being used was the media statement released on 5 May 2015, naming ‘Plus One Companions’ and its proprietors, Matthew Elliot and Travis Burch.26 An extract from the statement is as follows:

Plus One Companions advertises for ‘companions’ on websites including Gumtree and Seek. A telemarketer then phones the applicant and takes payment in exchange for listing on a database accessible only by members. Companions pay between $219 and $495 and are promised 4-6 inquiries per month from members seeking companions, and the chance to earn $150 an hour and up to $150,000 a year.
However, the investigation revealed Plus One Companions has no members, and no companions have ever received any work.

Fair Trading Active Exectuive Director Tony Johnson said the business was simply a sham and should be avoided.

The Australian Securities and Investment Commission

The Australian Securities and Investment Commission (ASIC) has a range of ‘facilitative, regulatory and enforcement powers’. Relevant to cold-call investment fraud is ASIC’s registration and regulation of companies, and their grants of Australian financial services licences.

In addition to those powers, other relevant powers include those associated with ASIC’s ability to investigate suspected breaches of the law. To progress those investigations, ASIC can require persons to produce books or have persons answer questions at an examination. ASIC also participates in national multi-agency taskforces.

Further, ASIC can ban persons from engaging in credit activities, or providing financial services. They can also issue infringement notices and take civil action.

In September 2014, the Commonwealth Parliamentary Joint Committee on Law Enforcement tabled their report in the House of Representatives and Senate, following an Inquiry into financial-related crime. Submissions received by the Committee included concerns around how effective ASIC was at acting on complaints. Ultimately, four recommendations were made that related to ASIC. In summary, those four recommendations are that:

- the Government review penalties relating to financial services legislation to achieve a better balance between non-compliance by licensed operators and unlicensed operations
- ASIC consider and then implement mechanisms to make its response to Internet-based financial related crimes far more expeditious
- the Australian National Audit Office conduct a performance audit of ASIC’s technological capacity
- ASIC strive to improve its relationships with the private sector in order to better detect and deter financial related crime.

The ASIC registration process is often considered by potential investors to signify that some assessment of the company or the licence-holder has occurred. The ACC reports that, in relation to the granting of Australian Financial Services (AFS) licences:

Regulation in the area of providing financial advice has tightened, but the AFS licensing process still has limitations. Although regulators conduct probity checks, which include police checks and bankruptcy searches on applicants for an AFS licence, it may be difficult to establish previous involvement in fraudulent activity either in Australia or in international jurisdictions.

[Unsuspecting investors may believe that due diligence has been performed by regulators in the granting of the licence, and that any money they invest will therefore be ‘safe’.

In reality, the steps to register a business name involve very basic provision of identification information, as provided on the ASIC website and shown below:

Enter your Australian Business Number (ABN)
Enter the proposed business name and registration periodEnter the proposed business name holder detailsEnter the addresses of the proposed business nameConfirm the eligibility to hold the proposed business name
Review your applicationMake your declarationsMake your payment [$34 for a year, $79 for 3 years]Confirmation
The eligibility step involves the business name holder declaring that they are eligible to hold a business name. Ineligible persons include any persons involved in the management of an entity who are disqualified from managing a corporation. An undischarged bankrupt remains eligible. Disqualified persons include those disqualified from managing a corporation under section 206B(1) of the Corporations Act 2001, as well as those convicted of an offence involving dishonesty, where the offence is punishable by imprisonment of at least 3 months (in this case, disqualification is for a period of five years from the date of release from prison, or from the date of conviction if the person did not serve a term of imprisonment). The onus is on disqualified persons to notify ASIC, by declaration. It is a criminal offence to make false and misleading statements in, or omit a material matter from, the application.

A consumer can search the ‘banned and disqualified’ list, which will bring up those persons disqualified by ASIC. As an example, Mario Girardo was sentenced to a term of imprisonment in Queensland in 2011, for offences including dishonesty. ASIC disqualified Girardo from managing corporations from 16 July 2012 to 15 July 2013. While he is no longer disqualified, the previous disqualification is displayed on a free and public search of the ‘banned and disqualified’ register.

Consumers can also search an ‘enforceable undertakings register’. Again, it means that ASIC has to have taken action, with the company agreeing to an undertaking, which is then published on the site.

ASIC claims to ‘promote investor and financial consumer trust and confidence’. However, the ASIC ‘register’ is essentially a list only, of all companies who have followed the above process. There is no obvious information on the ASIC website to alert members of the public that the bona fides of companies are not examined or assessed prior to registration. The international Financial Action Task Force (FATF) 2015 Mutual Evaluation Report (regarding Australia's anti-money laundering and counter-terrorism financing regime and compliance with FATF Standards) noted that 80 to 95 per cent of the companies registered with ASIC were registered online by a third party. Those third parties include lawyers and accountants, as well as trust and company service providers who specialise in company registration.

Despite that, ‘while ASIC does checks to ensure substantial compliance with lodgement obligations, it conducts only limited accuracy of information checks.’ Further, ‘no key information verification, including checks on criminal records or terrorist lists, is conducted. ASIC advised FATF that ‘if a registration contains suspicious elements or raises suspicion, more verification would be undertaken but that such a situation is very rare.’

The FATF concluded that while ‘Australia has implemented some measures to address the specific risk identified in the National Threat Assessment (conducted by the Australian Crime Commission [ACC]) to legal persons and legal arrangements, other measures need to be taken, including imposing AML/CTF obligations on those who create and register them in order to strengthen the collection and availability of beneficial ownership information.’

The Australian Government has responded to the FATF report by saying that the government ‘will look closely at the FATF’s findings, particularly as part of the statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 currently underway.’

Telemarketing and spam

The victims of financial crimes are almost invariably first introduced to the scam in which they ultimately invest by an unsolicited ‘cold-call’, or unsolicited email or other type of electronic message such as SMS, MMS or IM (instant messaging).

In Australia, messages sent to an email account, instant messaging account (IM) and telephone account (SMS and MMS) are covered by the Spam Act 2003 (Cth) and are regulated by the Australian Communications and Media Authority (ACMA). The Spam Act prohibits the sending of unsolicited commercial electronic messages and makes it mandatory for all messages to include a functional ‘unsubscribe’ message. The Act also prohibits the supply or use of address-harvesting software or the use or supply of an address list produced using address-harvesting software.
Telemarketing calls and faxes are covered by the Do Not Call Register Act 2006 (Cth). The purpose of this act is to prohibit unsolicited telemarketing calls and faxes to a number registered on the Do Not Call Register. Like the Spam Act, the Do Not Call Register Act is regulated by ACMA.

ACMA is the agency responsible for the enforcement of both Acts, and can take any of the following actions for breaches of either Act:

- issue a formal warning
- issue an infringement notice
- seek an injunction from the Federal Court
- prosecute a person in the Federal Court

It should be noted that these are civil remedies.

The Telecommunications Act 1997 (Cth) aims to promote responsible practices in relation to the sending of commercial electronic messages, the making of telemarketing calls, and the sending of marketing faxes. Under section 125A of the Telecommunications Act, ACMA was given a mandate to create industry standards for the telemarketing industry and the fax marketing industry.

The Telemarketing and Research Calls Industry Standard 2007 (Cth) sets out standards relating to the times when a telemarketer may call a consumer, specific information that a telemarketer must provide during a call, the termination of calls, and the requirement that telemarketers enable calling line identification.

Pursuant to the Telecommunications Act, ACMA has the power to appoint inspectors who may conduct searches relating to breaches of the Spam Act and the Do Not Call Register Act, or to monitor compliance with those Acts. The use of those powers might serve as a useful disruption tool.

The Australian Taxation Office and Taskforces

The Australian Taxation Office (ATO) investigates tax crime, which is said to be the abuse of tax and superannuation systems ‘through intentional and dishonest behaviour with the aim of obtaining a financial benefit’.

Serious tax crimes are generally prosecuted by the Commonwealth Director of Public Prosecutions, and summary offences under the Tax Administration Act 1953 (Cth) are prosecuted by the ATO.

The ATO works with law enforcement agencies to tackle serious and organised crime—particularly in identifying and combatting unexplained wealth. Information-sharing occurs to the extent allowed by law.

Case study

ATO uncovers organised money-laundering by identifying suspicious refunds

The following case comes from the ATO, which worked together with state police and the ACC to gather intelligence and, ultimately, dismantle a sophisticated network of organised crime:

We contacted a state law enforcement agency and the Australian Crime Commission (ACC) when our refund fraud analytical models identified suspicious GST refund patterns. A joint agency operation identified a financial adviser who was helping organised crime groups launder money through complex business structures.

Using their special powers, the ATO, state police and the ACC were able to gather specific intelligence on strategies designed to avoid tax and superannuation obligations, tax evasion through ‘phoenix’ activities, fictitious entities and cash-in-hand payments.
Based on the initial intelligence, the ATO was able to:

- identify, by working with law enforcement agencies, all of the financial adviser’s clients and potential links to organised crime entities
- compare the client base with those of other agents
- identify a number of entities not meeting their current lodgment obligations
- identify significant wealth accumulation through related entities
- compare the wealth of the private group to their tax performance to identify unexplained wealth.

This sophisticated organised criminal network was able to be dismantled because we worked with law enforcement agencies using a co-ordinated strategy. Twenty people were charged with multiple offences, including tax offences. Custodial sentences were significant, with up to nine-and-a-half years for the tax offences.

A number of civil sanctions were also applied as a result of subsequent audits, including tax assessments, with additional heavy penalties and director penalties. Debt collection strategies were also put in place, including garnishee notices, Mareva injunctions, and departure prohibition orders, to secure payment for the debts.

We also liaised with the Tax Practitioners Board to ensure that the financial adviser was deregistered and will be unable to practise again once released from prison.

The ATO is active in joint, national multi-agency taskforces. In particular, the ATO was the primary agency for Project Wickenby, a joint taskforce targeting people who promote and participate in the abuse of tax or secrecy havens. The ATO will also be leading two financial crime taskforces established in 2015: the Phoenix Taskforce and the Trust Taskforce. Further, a federal Serious Financial Crime Taskforce was established this year. The then-Federal Treasurer announced on 5 May 2015 that $127.6 million will be provided over four years for investigations and prosecutions that will address superannuation and investment fraud, identity crime and tax evasion. The taskforce includes the ATO, ACC, Australian Federal Police, Attorney-General’s Department, AUSTRAC, ASIC, Commonwealth Director of Public Prosecutions, and Australian Customs and Border Protections Services. The taskforce will build on the good work already done by Project Wickenby. During the course of Project Wickenby, $2.1 billion was raised in liabilities, as well as increased tax collections from improved compliance behaviour following interventions.

5.5.4 Police powers

Obtaining financial statements

The problem

The Commission was told that an impediment to investigating boiler-rooms (and other financial crimes) is significant delays (up to 18 months) in obtaining bank statements from financial institutions. This delay was also said to impact on the timely preparation of briefs of evidence and prosecution of matters, where charges have been laid prior to receipt of bank statements.

For example, the following three QPS officers describe the difficulties they have experienced in attempting to obtain bank statements from financial institutions:

- Detective Senior Sergeant Mitch Castles said investigators waited months for bank statements to arrive in relation to the Operation Juliet Dynamite investigation. In that matter, arrests were made...
prior to provision of the statements, because other evidence existed that indicated dishonesty. Arrests occurred in June 2012, with bank statements arriving in late 2012. An ACC financial investigator attached to the case could not complete the financial analysis until those statement arrived.52

- **Detective Superintendent Mick Niland** described waiting up to nine months for bank statements to arrive, creating a significant impact on investigators trying to deal with boiler-rooms. Once received, laborious work is undertaken to identify ‘money mules’ who have taken cash from bank accounts. He stated ‘you would think it would be quite easy to do a production notice, here’s a QPS production notice, you’ve got two weeks to hand it over, and it just doesn’t come.’53

- **Detective Superintendent Brian Hay** said generally it takes 3 months to get a bank statement, with QPS having no power to set a timeframe, whereas other states can demand records within a timeframe.54 Where four accounts required examination, it could be 12 months before all relevant bank statements were obtained. He further stated that ‘we can have a notice produced but it’s not enforceable if they don’t comply within the two weeks, and they simply don’t.’55

The problem is not universal across agencies and jurisdictions.

Both the Office of Fair Trading in Queensland and a representative of the New South Wales police force told the Commission that the turnaround after issuing a notice to produce financial records was often only a few weeks. Detective Inspector Phillip Roche of the NSW police said there was no undue delay obtaining bank records. He gave a specific example where notices to produce were served and records provided within approximately one week.56 Detective Inspector Roche noted that ‘the banks have their own law enforcement liaison area. Once you serve those notices on them, they will do whatever they can to serve the documents to police.’ In the example given, the documents were couriered to a local branch, and then collected by Detective Inspector Roche.

The Commission was told that requisition notices can be issued requiring banks to provide information to the Office of Fair Trading. While there had been occasional difficulties, responses generally arrived fairly quickly, with an estimated response timeframe of two to four weeks, unless voluminous material was requested.57

Section 90 of the *Fair Trading Act Qld 1989* contains the power to issue a notice. A requisition notice may require information or records to be furnished immediately at, by or within a time specified (section 90(3)(c) Fair Trading Act).

**Response of the “Big 4” banks**

ANZ stated that their average timeframe for responding to a warrant is 24 business days, and 8 calendar days for production notices. CBA provided their operating procedures, which included a provision to supply documents by fax or email, with a caveat that the documents are supplied to assist in a criminal investigation and are ‘not to be used for any other purpose (for example, court), without a search warrant or production order.’58 NAB told the Commission that their average timeframe for collating records sought under warrants or production notices is between two and eight weeks, depending on a range of variables—including the nature of the records, the date range and the date for compliance.

Westpac has recently introduced a ‘workflow controller’ within their Police Liaison Unit, who:

... records the due date of the notice into one of the Bank’s systems. If the due date is approaching and the request has not yet been complied with, a notification of the same is sent to the team leader who in turn follows up the bank officer.59 Since implementing this change in the last few months, 95% of requests from all agencies are within obligation date (being the due date for the request or, if no date is specified, 94 days after the request is received).60

All four banks operate centralised models, and so prefer production notices to be served on their registered office—if a notice is served on a local branch, the branch would send to the central office. There are different arrangements within each to respond to law enforcement requests for documents, but all had some form of compliance unit. NAB and Westpac told the Commission that they have dedicated police liaison email addresses to which requests can be made.
The ANZ, CBA, NAB and Westpac told the Commission the following in respect of the provision of electronic financial records:

**ANZ** told the Commission that it supports providing records electronically, and has done so since 2012, whereby records are embedded as PDF files on a CD-ROM. Whether they provide records electronically or by hard copy is determined by what it is the police officer has requested. 61

**Commonwealth Bank** stated that:

CBA has no policy against the provision of data via electronic means. Currently [the CBA] engage in electronic data exchange with a variety of state and federal agencies and statutory bodies and would be supportive of QPS progressing to [a similar arrangement]. 62

**National Australia Bank** stated that:

[C]onfidential information is not to be sent externally unless the information is encrypted. Common practice is for records to be produced on paper (this excludes call recordings and CCTV footage). Some staff have the capability to produce records via CD, DVD or USB which are password protected. Not all records are stored electronically and staff may need to retrieve the hard copy version. Staff have limited access to raw banking data and sometimes an imaged paper record is all they can retrieve. 63

**Westpac** stated that:

The Bank’s servers are only able to send emails externally with a size limit of 10MB. Accordingly, where the electronic version of material is less than this size limit, and the requesting party is content to receive documents electronically, material may be sent by email ... The Bank has a policy whereby the use of removable media devices including electronic storage devices is restricted, effectively meaning that material cannot be produced to law enforcement agencies by way of USB or CD unless in exceptional circumstances. 64

**The power to obtain financial records**

Financial records can be obtained by either of the following methods:

- applying for and executing a search warrant, sworn by a Justice of the Peace
- applying to a Magistrate for a Notice to Produce under sections 180–187 of the Police Powers and Responsibilities Act 2000 (Qld).

For QPS officers, the preference seems to be to obtain a search warrant. Since 1 January 2012, the QPS has only applied for 102 notices to produce. Conversely, in the same timeframe, 410 warrants were issued for records held by financial institutions. 65

In addition to obtaining search warrants and production notices, the Police Powers and Responsibilities Act provides for QPS officers to apply for the following:

- Production Orders (sections 188 – 195 of the Act)
- Monitoring Orders (sections 199 – 204 of the Act)
- Suspension Orders (sections 205 – 210 of the Act).

Since 1 January 2012, the QPS has not applied for any Production, Monitoring or Suspension Orders. 66 It is, therefore, not known how effective such orders would be in investigating or disrupting financial crime, or what the general approach courts have taken to making such orders.

Deputy Commissioner Ross Barnett told the commission, in relation to production notices:

[P]olice officers tend to utilise this investigative avenue less frequently than search warrants. This tendency is probably because the issuer for a production notice is a magistrate while a search warrant may be issued by a justice of the peace who are much more accessible. 67
It seems incongruous that a search warrant may be issued by a Justice of the Peace, where a production notice can only be issued by a Magistrate. Deputy Commissioner Barnett also highlighted this anomaly:

This threshold appears to be a policy anomaly given that a search warrant provides powers not conferred by a production notice, including search of the place and any [sic] anyone at the place. Consequently, a search warrant confers a potentially more intrusive power than a production notice.

The Commission recommends below that an application for a production notice, like a search warrant, should be able to be made to a Justice of the Peace.

**Timeframes**

There seems to be a misperception that production notices under the Police Powers and Responsibilities Act cannot set a timeframe within which financial institutions must comply. On the contrary, section 181(2) of the Act provides:

The magistrate may, in the production notice, require the documents to be produced to a police officer within a stated time and at a stated place.

The provision indicates that if information was placed before the Magistrate substantiating the need for a timeframe, the presiding magistrate could so order.

The Commission asked if any production notices containing a timeframe had been issued since 1 January 2012. No relevant data was able to be provided. Common practice in the QPS, in relation to both production notices and search warrants, is to wait until the relevant documents have been located by a financial institution and is ready for collection at a local branch. QPS will then have the search warrant sworn, or will make the application for the production notice.

In regard to production notices, Deputy Commissioner Barnett told the Commission:

Generally, an officer will advise an institution of an intention to obtain a production notice, and then wait for advice from the institution the evidence is available at a stated Queensland branch. The threshold for issuing a production notice is different to a search warrant in that the issuer only has to be satisfied the financial institution holds documents that may be evidence of an offence by another entity … However, an officer essentially relies on the co-operation of the institution, as under section 183 of the PPRA [Police Powers and Responsibilities Act] the institution does not commit an offence by failing to comply with the production notice.68

In regard to search warrants, Deputy Commissioner Barnett told the Commission:

… under section 151 Police Powers and Responsibilities Act 2000 (PPRA) a warrant may only be issued if the issuer is satisfied there is at a place or will be at a place in the next 72 hours the relevant evidence. The evidence sought for an investigation will often be held electronically by or for a financial institution and needs to be produced into a physical or paper form for evidence purposes. Such electronic information is generally held on a server in a central location often in another jurisdiction within Australia or overseas. Consequently, a police officer cannot obtain a search warrant until the officer is able to satisfy the issuer the documentary evidence is at a particular place within the territorial boundaries of Queensland.69

This approach was confirmed by ANZ and Westpac. ANZ told the Commission that they were usually notified by email of the scope of the proposed Warrant in advance of the Warrant being executed. Responsive materials are then prepared centrally and sent to a nominated ANZ branch for execution of the Warrant.70 Westpac stated:

There exists the following informal arrangement between the Bank and the QPS in relation to requests for material. The QPS will send an email to the Police Liaison Unit informing them that the QPS will be obtaining a warrant requiring the Bank to produce certain documents at a certain place and time in the future, thereby giving the Bank time to collate the necessary material. Once the material is collated, the Police Liaison Unit informs the QPS that the materials are ready and the QPS obtains the requisite warrant.
When asked about QPS executing warrants at a Queensland branch, NAB stated a preference for officers to notify the bank beforehand of the types of information and/or records sought, to allow sufficient time to collate records.71

Thus, there is no delay between when a search warrant or production notice is issued and when the evidence is obtained—the records are generally collected the same day.72 In those circumstances, the delay is actually between QPS advising a financial institution of an intended warrant/notice for records, and the arrival of those records at a place in Queensland. It is surmised that without a warrant or notice actually issuing, those requests do not carry any urgency and are not prioritised.

Responses from the ‘Big 4’ banks indicate that requests for records are generally prioritised by the ‘due date’ or ‘compliance date’ on the request:

**ANZ** stated that:

In the absence of a specified due/compliance date, requests are actioned according to an internally set timeframe depending on the size and complexity of the request.73 It is assumed that notices without a due date are not a high priority, although even if a timeframe is not provided on a notice or warrant, ANZ will do their best to fulfil a timeframe requested by the LEA [law enforcement agency] officer.74

**Commonwealth Bank** stated that:

Where requests had a clear due date, these due dates were adhered to wherever possible, where there was no clear due date the files were actioned in order of receipt.75

**National Australia Bank** stated that:

NAB’s prioritisation of LEA requests is based on its review of the request including the date of receipt and the compliance date specified, the urgency and nature of the LEA request, and any other relevant factors. The length of time to respond may vary depending on the type, volume and age of the records sought.76

**Westpac** stated that:

Documents are produced as requested, with a time and place for production having usually been nominated by the issuer.77

Not surprisingly, banks appear to prioritise notices and warrants according to their due dates. A Law Enforcement Agency (LEA) request without a timeframe is likely to be given a lower priority. In light of the QPS interpretation of section 151 of the Police Powers and Responsibilities Act, QPS cannot execute a search warrant until the records are geographically within Queensland and are thereby restricted in setting a timeframe. A production notice does not require records to be physically at a Queensland branch:

The threshold for issuing a production notice is different to a search warrant in that the issuer only has to be satisfied the financial institution holds documents that may be evidence of an offence by another entity. Consequently, the documents need not be within the territorial limits of Queensland.78

Thus, it would be preferable if production notices were served on banks at the time of the request for records, with a set timeframe. It seems unlikely that QPS will adopt that practice while production notices continue to require applications to a magistrate.

It is therefore recommended below that the Police Powers and Responsibilities Act be amended to allow applications for production notices to be made to a Justice of the Peace or a Magistrate.

The use of production notices will allow QPS officers to nominate reasonable timeframes in applications, prior to serving the notices on financial institutions—in a way that will increase efficiency.
Confiscations: Criminal Proceeds Confiscation Act 2002

The legislative framework for the confiscation of proceeds of crime in Queensland is governed by the Criminal Proceeds Confiscation Act (Qld). That Act provides three schemes for the confiscation and forfeiture of property and money, as the chapter on an organised crime specific offence, below. For present purposes, a summary of those schemes is as follows:

- **Chapter 2** of the Act is administered by the Crime and Corruption Commission (CCC) and allows for the confiscation of assets, whether or not a person has been convicted of any offence or even charged. Chapter 2 includes the ‘unexplained wealth’ provisions that enable the Court to order the confiscation of a person’s assets, unless the person can prove those assets were lawfully acquired.

- **Chapter 2A** of the Act, also administered by the CCC, provides the Serious Drug Offender confiscation order scheme.

- **Chapter 3** of the Act is currently administered by the Office of the Director of Public Prosecutions, and applies only after a person has been charged and convicted of a ‘confiscation offence’, which includes an indictable offence punishable by at least five years imprisonment (including fraud).

An issue relating to victims of fraud

The net proceeds of property forfeited under Chapter 2 of the Act (including unexplained wealth orders) must be paid into consolidated revenue. There is no mechanism for distribution of property which is the subject of an ‘unexplained wealth order’ to victims of the ‘serious crime related activity’ that formed its basis.

After conviction, the scheme in Chapter 3 of the Act provides for restraining orders, forfeiture orders and pecuniary penalty orders to be made in respect of benefits derived from, and anything used for, the commission of a ‘confiscation offence’. Again, fraud constitutes a ‘confiscation offence’.

The effect of a post-conviction forfeiture order under Chapter 3 of the Act is that the property which is the subject of the order is forfeited to the State and vests absolutely in the State. Payment under a pecuniary penalty is also to the State.

Although the Attorney-General has power under the Act to give directions about how property forfeited under the Act is to be dealt with, the CCC notes that ‘there is no mechanism under the Act to permit recovery by or on behalf of another party’.

Gaps and inadequacies

As mentioned above, Chapter 2 of the Criminal Proceeds Confiscation Act is invoked prior to conviction, when ‘victims’ could have no claim to a suspect’s property other than by a judgement in civil proceedings. Any such proceeding against a suspect would be futile if the property had vested in the State subject to an ‘unexplained wealth’ forfeiture order. Alternatively, the claim would have to be made against the State. Further, it would not be appropriate for the Act to create a regime for the compensation of ‘victims’ where there has not been a conviction.

That, however, does not and should not prevent law enforcement agencies from seizing money and other property when that option is appropriate and authorised as part of a crime disruption or investigation process. If, in the end, there is no conviction and no order for forfeiture of seized money, the money and/or property...
Financial Crimes

must be returned to a suspect. In that case, as costly and complicated as it might be, those who claim to have suffered loss maintain the option of taking civil action to recover their investment.

The Commission considers that the situation after conviction is different, and that there is scope for legislative reform designed to enable victims of serious fraud offences to recover financial loss occasioned by the fraud. The CCC supports a proposal for such reform.84

The Victims of Crime Assistance Act 2009 only applies to victims of crimes against the person. It aims to provide financial assistance to assist victims of crime recover from acts of violence.85 A review of that Act was commenced in November 2014 with consultation sought in respect of possible reforms ‘across three key themes’:

- financial assistance scheme for victims
- the fundamental principles of justice for victims
- the role of the Victim Services Coordinator and how to resolve complaints related to the fundamental principle of justice.

The terms of reference for the review do not allude to any consideration of broadening the scheme to include assistance for victims of other types of crime, including financial crime.86 The Commission is not apprised of the progress of that review.

The CCC points out that a number of government departments maintain ‘fidelity funds’, used to pay victims who have suffered loss on account of contraventions of particular laws.87 A similar fund might be considered to allow victims of serious frauds to make application for compensation, after (an) offender(s) has been convicted in respect of the fraud(s). That is, funds that would ordinarily vest in the State as a result of an order under Chapter 3 of the Criminal Proceeds Confiscation Act would be made available for victims capable of satisfying certain criteria for compensation.

In considering such a scheme, the CCC suggested that the following factors should be considered:

- whether the fund should be administered by the CCC or an agency independent of the confiscation process
- a threshold for access to the fund (for example, only for fraud amounting to more than a particular sum of money) and whether the scheme should only apply to a ‘serious fraud’ as defined by the legislature
- policy implications of using State resources to recover funds for victims of fraud.88

The Commission agrees that those are important matters for consideration, and that a broad consultation process would be necessary before the implementation of such a significant reform.

Recommendation

5.9 The Commission recommends that the Queensland Government consider establishing a scheme to allow the victims of serious frauds to apply for compensation from property forfeited to the State under Chapter 3 of the Criminal Proceeds Confiscation Act 2002.

(Endnotes)

1 (Unreported), Southport District Court, O’Brien CDCJ, 30 July 2015.
2 Commissions of Inquiry Order (No.1) 2015, para 3(g).
4 For example, State of Tasmania v Williams, 25 September 2015, ‘Comments on passing
5 Financial Crimes


6 R v Morehu-Barlow [2014] QCA 4 at para [29].

7 R v Morehu-Barlow [2014] QCA 4 at [25] [relying on R v Heiser & Cook; ex parte A-G (Qld) [1997] QCA 14, p. 5].

8 [2012] QCA 43.

9 [2013] QCA 327.

10 Section 8 Vicious Lawless Association Disestablishment Act 2013 (Qld).

11 Section 5 Vicious Lawless Association Disestablishment Act 2013 (Qld).

12 Statutory Declaration of Terry Lawrence, 28 August 2015, para 52.

13 Statutory Declaration of Michael Byrne QC, 10 September 2015, paras 2–4.

14 Statutory Declaration of Terry Lawrence, 28 August 2015, paras 54–55.

15 The Commission notes the role of the Taskforce, and that the Criminal Organisation Act 2009 expires on 15 April 2017 and must be reviewed this year.


17 Section 1 Criminal Code.

18 Section 1 Criminal Code.


20 Hansard, 9 February 2010, p. 100.

21 Hansard, 9 February 2010, p. 90.

22 Statutory Declaration of Terry Lawrence, 20 August 2015, para 3, pp. 1–2.

23 Transcript of interview, Steve L’Barrow, p. 20.

24 Transcript of interview, Steve L’Barrow, p. 21.

25 Transcript of interview, Steve L’Barrow, p. 21.


32 ‘person involved in the management of an entity’ is defined as those who are involved in making decisions that affect the whole or a substantial part of the entity or have the capacity to affect significantly the entity’s financial standing.


38 Part 7, Section 41 Spam Act 2003 (Cth); Part 6, Section 40 Do Not Call Register Act 2006 (Cth).
458 Queensland Organised Crime Commission of Inquiry

39 Schedule 3, Section 30 Spam Act 2003 (Cth); Schedule 3, Section 32 Do Not Call Register Act 2006 (Cth).

40 Part 5, Sections 31–36 Spam Act 2003 (Cth); Part 5, Sections 33–38 Do Not Call Register Act 2006 (Cth).

41 Part 4, Sections 23–29 Spam Act 2003 (Cth); Part 4, Sections 23–30 Do Not Call Register Act 2006 (Cth).

42 Section 27 Spam Act 2003 (Cth).

43 Section 3 Telecommunications Act 1997 (Cth).


51 Transcript of hearing, Brian Hay, 21 July 2015, lines 35–45, p. 159.

52 Transcript of hearing, Mitch Castles, 20 July 2015.

53 Transcript of interview, Mick Niland, 2 July 2015, p. 5.

54 Transcript of interview, Brian Hay, 19 June 2015, pp. 11–12.


56 Transcript of hearing, Phillip Roach, 21 July 2015, lines 40–45, p. 121.

57 Transcript of interview, Steve L’Barrow, 30 July 2015, p. 11.


60 Statutory Declaration of Louise Condon, 30 July 2015, para 53.

61 Telephone call with Shaq Johnson, 30 July 2015, 2968277.

62 Statutory Declaration of Stephen Harley, 21 July 2015, para 2, item 5.

63 Statutory Declaration of Kristy Haidar, 5 August 2015, para 8.

64 Statutory Declaration of Louise Condon, 30 July 2015, para 35–36.

65 Statutory Declaration of Ross Barnett, 5 August 2015, para 2.


67 Statutory Declaration of Ross Barnett, 5 August 2015, para 7.

68 Statutory Declaration of Ross Barnett, 5 August 2015, para 8.

69 Statutory Declaration of Ross Barnett, 5 August 2015, para 3.

70 Statutory Declaration of Shaq Johnson, 30 July 2015, para 2.1.3.

71 Statutory Declaration of Kristy Haidar, 5 August 2015, para 9.

72 Statutory Declaration of Ross Barnett, 5 August 2015, paras 4, 10.

73 Statutory Declaration of Shaq Johnson, 30 July 2015, para 2.3.

74 Telephone call with Shaq Johnson, 30 July 2015, 2968277.

75 Statutory Declaration of Stephen Harley, 21 July 2015, para 2, item 2.

76 Statutory Declaration of Kristy Haidar, 5 August 2015, para 5.

77 Statutory Declaration of Louise Condon, 30 July 2015, para 12.

78 Statutory Declaration of Ross Barnett, 5 August 2015, para 8, p. 4.

79 Section 214(5) Criminal Proceeds Confiscation Act 2002 (Qld).

80 Section 94 Criminal Proceeds Confiscation Act 2002 (Qld).
5.6 Responses to organised crime

5.6.1 Queensland law enforcement

The Queensland Police Service (QPS) submission to the Commission outlined the policing response to organised crime—noting that the response is focused on the substantive crimes as well as the enablers of organised crime.\(^1\) The nature of the policing response to organised crime is said to be two-fold:

1. intelligence-based tactical approaches, including national arrangements that target organised crime through law enforcement on a priorities-and-risk basis (supply reduction)
2. preventative strategies, such as education and community engagement (demand reduction).

Intelligence-based tactical approaches to organised crime are made ‘at the local policing level and through nationally coordinated strategy implemented through joint taskforces and operations.’\(^2\)

Information-gathering and sharing is achieved through the CrimTrac agency in Canberra, specifically through the use of the CrimTrac National Police Reference System. That system, along with the QPS Queensland Police Records and Information Management Exchange (QPRIME) system and new mobile technology, allows intelligence to be built through otherwise-disconnected pieces of information.

The QPS also told the Commission that it delivers services ‘around organised crime through various dedicated policing groups based in the south east of the state as well as at the local/regional level.’\(^3\) Following that statement, the submission listed the following dedicated policing groups:

- Drug and Serious Crime Group (including the State Drug Squad, Organised Crime Investigation Unit, Townsville and Cairns Drug Squads, and Gold Coast Major and Organised Crime Squad)
- Operation Resolute (comprising Taskforce Maxima and Takeback)
- Child Safety and Sexual Crime Group (including Taskforce Argos)
- State Intelligence Group.

The Drug and Serious Crime Group and the Child Safety and Sexual Crime Group fall within the State Crime Command, along with the Homicide and the Fraud and Cyber Crime Group (FCCG). Curiously, no mention was made of the FCCG in the QPS submission regarding the policing response to organised crime; however, the FCCG has an investigation function (including assisting the response to cyber attacks against the Queensland Government), a regional assistance function, and a prevention function.

The purpose of the State Crime Command is to ‘provide focused, high level, proactive investigative expertise targeting serious and organised crime.’\(^4\)

---

81 Section 153.
82 Section 184(1)(b) and section 184(4).
84 Statutory Declaration of Angela Pyke, 7 September 2015, para 71.
85 Section 5 Victims of Crime Assistance Act 2009.
87 Submission of the Crime and Corruption Commission, May 2015, p.71, citing the Office of Fair Trading (for contraventions of the Fair Trading Act 1989) and the Department of Natural Resources and Mining (for contraventions of the Land Title Act 1994) as examples of existing fidelity funds.
The State Crime Command Priorities Statement for 2014–2015 includes ‘targeting high level individual and network criminal activities utilising Specialist Investigative strategies.’ The other stated priorities are to:

- partner in local, national and international efforts in addressing serious and organised crime
- create a diverse and flexible service delivery model through the application of case and place management strategies
- increase productivity and performance through a managed program of projects
- promote a climate to encourage ethical and professional leadership and effective decision-making. 5

The Terms of Reference directed the Commission to report on:

- Gaps within the knowledge of Queensland law enforcement agencies of the crime environment and to suggest priority areas for intelligence collection;
- The responses of law enforcement, intelligence and prosecution agencies to maximise the reduction of risk to the community of Queensland and to prevent, disable or disrupt activities of organised crime; and
- The adequacy of legislation and resources available to law enforcement and intelligence and prosecution agencies to effectively address organised criminal activity.

In the process of learning about the burgeoning problem of fraudulent cold-call investment schemes operating on the Gold Coast, it became evident that there is a serious and long-standing problem with the way police have responded to them. The Commission also found that there is scope to improve the way that the QPS prioritises the work involved in addressing organised crime (whether it be through prevention, disruption and/or investigation) through a more focused use of intelligence resources, and better resourcing.

Strategies for addressing organised crime

The QPS acknowledges that a coordinated response across jurisdictional boundaries is necessary to address modern organised crime. It cites the emergence of new technologies, information-sharing between law enforcement agencies within Australia and overseas, and the need for coordinated national and transnational responses as operational challenges.

Those challenges are said by the QPS to be recognised by the development of the National Organised Crime Response Plan 2010–2013 (NOCR Plan) with its ‘focus on improving the interoperability and information sharing between the states and the Commonwealth, targeting the criminal economy, improving operations responses, prevention and international and domestic partnerships.’ On 22 May 2015, the national Law, Crime and Community Safety Council endorsed the NOCR Plan for 2015–2018.

The most recent NOCR Plan outlines six initiatives directed at making ‘a tangible impact on the key organised crime threats facing Australia.’ Three of those six initiatives are relevant to financial crime, with a fourth dealing with the importance of cross-jurisdictional information sharing:

- Initiative 3 – targeting organised crime groups committing technology-enabled crime
- Initiative 4 – developing a strengthened approach to financial crime
- Initiative 5 – tackling the criminal proceeds of organised crime
- Initiative 6 – reducing barriers to information-sharing between agencies

The rationale behind the addition of the financial crime initiative is the increasing threat of serious and organised crime to the financial sector and to the integrity of the economy, the diverse nature and scale of financial crime, and the new opportunities available through a globalised economy and advancements in technology. Australia’s lucrative superannuation pool is also seen as an attractive market for crime syndicates.

The NOCR Plan also recognised that there are intelligence gaps in respect of the extent of the problem of organised financial crime, with ‘the intermingling of licit and illicit financial transactions [making] it difficult to fully gauge the extent of these activities.’ 7
The NOCR Plan provides examples of successful cross-agency task forces that have tackled different aspects of financial crime—including Project Wickenby (targeting tax evasion) and, relevantly, Taskforce Galilee (targeting boiler-room fraud). Taskforce Galilee is said to have helped disrupt this type of criminal activity and better educate Australians about the threat it poses. The NOCR Plan notes that this type of fraud is often based offshore; it does not allude anywhere to the serious problem of boiler-room frauds operating onshore, in Queensland.

The NOCR Plan is not specifically recognised in current QPS strategic planning or in priorities documents, and—perhaps more importantly—the QPS does not have a strategic plan for responding to organised crime. Rather, the QPS says that it ‘incorporates aspects of organised crime into its general crime response strategies.’ That is justified by the QPS on the basis that organised crime is one of many priorities, and that the QPS Operational Plan 2014–2015 has identified a range of organised-crime-related activities that are aligned to the NOCR Plan. The QPS Operational Plan includes ‘working closely with Commonwealth law enforcement agencies and intelligence agencies and targeting high level individual and network criminal activities.’ The Commission was not told whether or not, or to what extent, the QPS will be involved in developing a national approach to targeting financial crime as prioritised by the NOCR Plan.

The Senior Officers’ Group on Organised Crime and the Serious and Organised Crime Coordination Committee are avenues through which to do that. The Senior Officers’ Group on Organised Crime is comprised of senior officers, and it performs a governance role in respect of the NOCR Plan. The Serious and Organised Crime Coordination Committee is comprised of representatives of State and Commonwealth law enforcement agencies, the Australian Crime Commission (ACC), Customs, and the Australian Taxation Office. It is said to progress operational and intelligence-led initiatives.

The Senior Officers’ Group on Organised Crime and the Serious and Organised Crime Coordination Committee are the key bodies for coordinating strategic, operational and tactical responses to organised crime on a national level. Although mention is made of both groups in the QPS submission to the Commission, the extent of QPS engagement in them remains unclear.

Involvement in those groups and engagement in the national response to the threat of serious and organised crime is clearly essential, given the recognition by the QPS that there is a ‘need for a coordinated national and increasingly, transnational response to organised crime in Australia.’

Another strategy for improving the way law enforcement deals with organised crime has been developed by officers of the QPS, but not yet adopted by State Crime Command. This new strategy is the Criminal Economy Strategy, which aims to capture the hierarchy of criminals operating in networks by focusing attention on the wealth generated by criminal organisations, rather than on the crimes committed to generate it. It is a strategy that accords with current thinking about more effective ways to disrupt and dismantle organised crime networks. For example, the NOCR Plan Initiative 5 dealing with the proceeds of crime states that:

Most organised crime is motivated by profit. Attacking the profit that motivates and finances organised criminal activity is a highly effective means of disrupting serious and organised crime networks and reducing the harm they cause. This can be achieved through targeting criminals’ laundering operations, pursuing proceeds of crime and make full use of unexplained wealth laws.

The ‘Criminal Economy Strategy’ has been employed as a kind of pilot program by the Criminal Economy Unit of Taskforce Maxima. It was that unit that has led the joint operations between the QPS and the Queensland Crime and Corruption Commission (CCC) in targeting boiler-rooms with some apparent success.
Intelligence and monitoring of financial crime

The Commission was informed that there is a concern that the QPS is often complaint-led rather than intelligence-led when it comes to responding to organised crime.\(^{13}\) To the extent that this is the case, it is concerning—given the perennial problem of allocating finite resources appropriately.

The QPS has numerous resources available to it to properly inform itself about crime trends and particular areas of concern. Internally, the State Intelligence Group is responsible for delivering intelligence services to the QPS by providing intelligence products to support decision-making at tactical, operational and strategic levels.\(^{14}\) Intelligence officers also work with other agencies in the Queensland Joint Analysis Group and in joint task forces. The Joint Analysis Group became a permanent unit of the QPS in May 2015.

The Target Development Unit and the Operations Register are other internal resources that are said to assist in the identification and analysis—including risk assessment—of organised crime networks in Queensland, in order to prioritise resource allocation.\(^{15}\)

The ACC holds the National Crime Target List (also referred to as the ‘NCTL’), which includes ‘nationally significant organised criminal syndicates and individuals’. The National Crime Target List is said to inform ‘jurisdictional priorities with respect to prevention and intervention activities, including Queensland.’\(^{16}\) The QPS contributes to the development of the National Crime Target List along with other law enforcement agencies across the country. The State Intelligence Group of the QPS sits on the Australian Criminal Intelligence Forum in order to do that.

The mandate of the Australian Criminal Intelligence Forum is to implement the Australian Criminal Intelligence Model. That model recognises that ‘an intelligence-led approach is fundamental to the success of the national response to organised crime,’ and it ‘aims to achieve the free flow of intelligence between policing, law enforcement, and regulatory and national security agencies, based on consistent standards, processes and protocols.’\(^{17}\)

The QPS submission to the Commission sets out a diagram showing the complex integration of QPS intelligence capabilities with national arrangements:
OCRA (previously TITAN) QPS organised crime risk assessment measures organised crime attributes, including intent and capacity to commit serious crime. OCRAs are a function of the Qld Operations Register.

TRAM – ACC Target Risk Assessment Methodology aims to manage serious and organised crime risks based on consideration of targets’ threat and impact at a national level.

According to the diagram, intelligence should filter through to a covert and/or targeted operation in the case of an identified ‘high threat’, or to the State Crime Command investigation groups (presumably for investigation). It is clear that the strategy has not worked—or has not worked well—in respect of cold-call investment frauds.

The Commission was provided with an intelligence assessment, current as at January 2015, regarding boiler rooms thought to be operating on the Gold Coast. Based on other information provided to the Commission from various sources, it is considered more than likely that that intelligence product was deficient then, and almost certainly outdated now. If resources are to be properly allocated, and if organised crime in Queensland is to be properly addressed, then it is critical that up-to-date and accurate intelligence be available.

Recommendation

5.10 The Commission recommends that the Queensland Police Service prioritise cold-call investment frauds for intelligence collection. The Queensland Police Service State Intelligence Unit be properly resourced to produce a detailed intelligence report regarding cold-call investment frauds operating in Queensland.
Cross-jurisdictional arrangements and cooperation

Information-sharing is imperative to successfully combating organised crime, including financial crime.

In the absence of information-sharing, law enforcement may not be able to identify the existence of multiple victims in multiple locations, and they may treat a matter as a one-off offence. It is difficult for general duty police officers to ‘police their beat’ by building knowledge around cybercrime perpetrators, because the offences are so often cross-jurisdictional and enabled by other crime.

A number of examples were provided to the Commission of investigations involving cooperation with other agencies. It is evident from those examples, and from other information provided to the Commission, that the QPS has developed some effective partnerships to assist in targeting financial crimes in an increasingly borderless environment.

Card-skimming and money-laundering operations

The case study above involving Stroia and his associates provides an example of a successful operation targeting a card-skimming and money-laundering operation. The Proceeds of Crime Group within the QPS FCCG commenced Operation Kilo Dictate in March 2012, after the Australian Transaction Reports and Analysis Centre (AUSTRAC) identified a number of suspicious transactions.

Operation Kilo Dictate resulted in the arrest of 28 offenders, who were mainly Romanian nationals with some suspected connection to Russian crime syndicates. It highlighted the importance of information-sharing and transnational cooperation: Through Interpol and Europol, and with the assistance of the Australian Federal Police (AFP), information was disseminated to police in London as well as the Romanian Fraud Taskforce (where offenders had been identified by the QPS). The QPS also noted the assistance of money remitter Western Union in the success of the operation.18

Also in 2012, Operation Lima Matlock targeted sophisticated card-skimming schemes organised by a man named Hennessy and facilitated by others, who performed various roles—both within Australia and overseas. Operation Lima Matlock was coordinated by the Major and Organised Crime Squad on the Gold Coast.19

Operation Lima Matlock involved information-sharing and cooperation with other Australian law enforcement agencies and Australian Customs. Intelligence was also shared with police in the United Kingdom and New Zealand.

The QPS, through Taskforce Maxima’s Criminal Economy Unit, continues to target card-skimming schemes, with the assistance of the AFP as well as interstate and overseas law enforcement agencies. Western Union also continues to assist.20

Advance-fee frauds and romance scams

Advance-fee frauds and romance scams typically involve overseas-based offenders; therefore, targeting offenders requires the assistance of international law enforcement agencies. The QPS has been involved in at least one successful operation that resulted in the arrest of fraudsters in Ghana, with the help of local law enforcement. The Federal Bureau of Investigation (FBI) and the United States Postal Service—as well as police in the United Kingdom—have also provided assistance in the investigation of advance-fee fraud committed against Queensland residents.21

One problem encountered by police in dealing with this type of financial crime is that complainants sometimes refuse to believe that they have been scammed. In one case, an elderly woman was scammed by a man in the United States, but refused to accept that the purported romance was a sham. The QPS provided support to her family members, who had tried in vain to stop the woman sending more money. The FBI located the offender, but was unable to charge him, since the victim would not make a complaint. Ultimately, the Queensland Civil and Administrative Tribunal, on an application made by the woman’s son, made an order appointing the Public Trustee as administrator of the woman’s financial affairs.22

An additional challenge for law enforcement is that these types of scams are increasingly being operated from Malaysia, where the high legitimate money flow makes it more difficult to identify possible victims.23
Whereas in the past, with information provided by AUSTRAC, the QPS could analyse each transfer of money from a Queensland resident to Ghana or Nigeria in order to alert potential victims, this is not possible with the volume of transactions in the Malaysian markets.

**AUSTRAC**

The role of AUSTRAC in tackling organised crime is dealt with in some detail in the following chapter on Money laundering.

AUSTRAC provides important resources to the QPS, which has an AUSTRAC officer embedded in the FCCG. Beyond providing information about transactions to high-risk locations around the world, AUSTRAC assists the QPS by:

- providing consultation and direction with investigations
- assisting in planning and execution of investigations
- assisting with analysis of particular financial searches
- tracing money from the point of origin as far as can be identified
- assisting with building a picture of persons of interest from the financial information, such as suspicious transaction reports.

**The Australian Cybercrime Online Reporting Network and the National Plan to Combat Cybercrime**

Mention has also been made of the Australian Cybercrime Online Reporting Network (ACORN), a national policing initiative borne out of the National Plan to Combat Cybercrime. ACORN, along with Project Synergy (discussed in more detail below), are the two initiatives outlined by the QPS in describing the ‘proactive approach to fraud and cyber-crime.’

The ACORN website allows members of the public to securely report instances of cybercrime, and also provides information about how to recognise scams and advice to those who have fallen victim.

The National Plan to Combat Cybercrime commits Australian governments to taking concrete steps under six key priorities:

- educating members of the community to protect themselves
- partnering with industry to tackle the shared problem of cybercrime
- fostering an intelligence-led approach and better information-sharing
- improving the capacity and capability of our agencies to address cybercrime
- strengthening international engagement on cybercrime
- ensuring our criminal justice framework keeps pace with technological change.

According to the QPS, the ACORN initiative appears to be effective in facilitating the reporting of cybercrime offences, with 9,680 complaints made to police nationally during the period 1 January 2015 to 31 March 2015, approximately 107 complaints every day. In that first quarter of operation, $234 million worth of financial loss was reported by victims. Alarmingly, Queensland receives the second-largest percentage of complaints (22 per cent), only slightly less than Victoria (23 per cent).

The success of ACORN in bringing cybercrime to the attention of police has brought with it the challenge of resourcing the response. When ACORN was first introduced in November 2014, the expectation was that the QPS would receive something in the order of seven or eight complaints per week. The reality has been an average of 33 complaints per day.

The Cybercrime Investigation Unit within the FCCG of the QPS currently has responsibility for triaging that large volume of ACORN-generated complaints, assigning investigations and passing information to the AFP where appropriate. Before a matter can be assigned or investigated, it is incumbent on officers from the Cybercrime Investigation Unit to undertake preliminary investigations (which might take a number of days) to ascertain jurisdiction. Frauds that appear to originate overseas are reported to the AFP, which is responsible for intelligence-sharing with overseas law enforcement agencies.
Recommendation

5.11 The Commission recommends that the Queensland Police Service Fraud and Cyber Crime Group be appropriately resourced to deal with the much higher than expected volume of complaints referred to the police through the Australian Cybercrime Online Reporting Network.

Addressing organised financial crime: boiler-rooms

In its initial submission to the Commission, the QPS did not raise either the extent of the organised crime problem or the inability, for whatever reason, to address it. In its later submission addressing evidence received during the course of the Inquiry, the QPS maintained that the FCCG has, in general, adequately responded to complaints from persons claiming to have been defrauded by boiler-rooms.29

Information and evidence provided to the Commission was to the contrary.

The Commission commenced its inquiry into the response of the QPS in dealing with organised financial crime by interviewing Detective Superintendent Brian Hay on 19 June 2015. Prior to commencing an extended period of leave in July 2015, Detective Superintendent Hay led the FCCG, and had done so for almost 12 years.

Detective Superintendent Hay told the Commission that:

- The fundamental reason why some cold-call investment fraud complaints have not been investigated is a lack of resources: ‘[T]here’s more fraud than there are police officers to respond to it, bottom line.’30
- Investigations of alleged cold-call investment fraud are ‘extremely intensive and difficult to do.’31 Such investigations take a long time and there is a concern that the longer an investigation goes on, the more victims fall prey to the scam.32
- Time is of the essence in the investigation of cold-call investment frauds. The time it takes to obtain bank statements (from three months and up to two years33) is ‘extremely frustrating’ and it hampers investigations.34
- The FCCG had investigated a number of boiler-rooms ‘over the years’ during the course of a number of operations.
- One such operation involved disruption strategies and resulted in the fraudulent scheme bring shut down. It was described as a ‘big learning curve.’35
- It is ‘absolutely’ preferable to focus on disruption rather than investigation and prosecution.36
- Most detectives do not want to investigate fraud, and that results in ‘duck shooting and flicking’ with reference to matters being sent in to the FCCG from the regions.37
- The fraud squad has traditionally been a ‘dumping ground’ for officers who are unenthusiastic about and/or inexperienced in the type of work, and who are eager to leave as soon as the opportunity presents.38 That has changed recently, when the fraud squad was able to advertise for positions so that those who applied for the jobs wanted to be there. That recruitment drive resulted in the addition of six ‘really good people’. That has only happened in the last six months.39
- The FCCG allocated more than 20 people to Taskforce Maxima to deal with outlaw motorcycle groups.
- There are currently a number investigators in fraud.40 Officers are regularly diverted to matters involving investigations for political matters, including fraud against the Government (as in the case of...
Financial Crimes

Queensland Organised Crime Commission of Inquiry

Detective Superintendent Hay said, ‘we [FCCG] get sucked more and more and those political imperatives take over and sometimes work gets left on the shelf, sadly but it’s true. It is a constant balancing act and an issue of priority and analysis.’

- Rather than persisting with a ‘long, tedious, expensive process’, Mr Hay wants to develop a strategy that involves ‘short, sharp incursions, disruption strategies and prosecution technique.’

- Attacking the criminal economy of organised crime is a strategy aimed at working from the top of an organisation down, rather than the traditional method of investigation from the bottom up. The rationale is that organised crime is not about drugs, for example. It is about making money.

- The QPS is complaint-led, rather than intelligence-led, and there is a long way to go on that front.

- For an intelligence-led disruption strategy to be effective, it is necessary to build networks involving the private sector. For example, web designers, graphic designers and local printers who are engaged to print the glossy brochures for cold-call investment frauds could assist to feed intelligence about new schemes to the police.

- A multi-agency (including industry) task force is necessary in order to effectively disrupt boiler-rooms. Detective Superintendent Hay has been agitating for the establishment of such a task force for some time. It would include skill sets designed to address the crime type, including appropriately skilled police, accountants and technical experts. The task force might also involve the assistance of the Office of Fair Trading and the Australian Securities and Investments Commission (ASIC).

- A strong media campaign for public awareness is essential.

- However, people who complain to the media and politicians about police inaction serve to distract resources from where they should be directed. And further, as to complaints of inaction:

  We get that all the time, people aren’t happy with the outcome. We rely on evidence, they still have the right to proceed in a civil proceeding should they wish but there is not enough weight of evidence for us to go forward. And of course, we must be corrupt, we are just lazy. It is a constant battle and the time we spend responding to ministerial briefs and these sorts of complaints is just a distraction from core business. But, I suppose it is part of core business now but it is something we have to deal with all the time.

The impression was that Detective Superintendent Hay has many good ideas but that very little, if any, progress has been made toward implementing them.

Through media reports, it became evident that Mr Ken Gamble, a private investigator, had been agitating for action by the QPS on behalf of a number of complainants for many years.

Mr Gamble made a written submission to the Commission in order to highlight his views about the growing problem of serious and organised investment fraud on the Gold Coast, and the lack of response by the QPS Fraud Squad (the FCCG) to these serious frauds.

The submission provided two case studies to demonstrate the problems encountered in dealing with the FCCG. One of those matters involves an alleged boiler-room that is yet to be investigated by police (referred to as ‘the 2011 complaints’), and the other involves a matter currently before the court. While the Commission is unable to have regard to the substance of the latter, and does not wish to compromise any future investigation into the former, the general observations made by Mr Gamble were useful to understanding the nature and extent of the problem within the QPS. The Commission has only had regard to the investigation of those matters, not to any matter of substance or the merits of any case.

Mr Gamble observed that, since as early as 2009, he has had personal experience in dealing with the frustration of fraud victims and interstate police in trying to have their cases investigated by the QPS. Common complaints centre on a lack of communication from the QPS, and lack of action in response to complaints.
Mr Gamble has used the media several times as a platform to draw attention to serious fraud cases that seem to have been ignored by the QPS. He has also, on occasion, suggested that approach to complainants. That strategy led to ‘an even further disconnection’ between the QPS and the victims. Mr Gamble concluded (correctly, as the evidence ultimately showed) that he, and those he represented, were perceived as troublemakers and a nuisance to the FCCG.

As to the cause of the problem, Mr Gamble said that the FCCG ‘appeared to have little to no capacity to investigate Internet related fraud despite the extensive publicity campaigns organised by Detective Superintendent Hay.’

Mr Gamble later made himself available to speak with the Commission to answer specific questions about matters raised in his submission. Mr Gamble was robust and direct in his criticisms of the QPS; however, his observations were tempered with appropriate concessions and acknowledgement of good work where it was due.

Hearings were held in order to further investigate the nature and extent of boiler-rooms on the Gold Coast, as well as the issues regarding the QPS response to them. The hearings were held in camera given that the areas of inquiry necessarily involved questions regarding matters currently the subject of judicial proceedings, as well as details of current and anticipated intelligence collection strategies and investigation methods.

The Order in Council precludes the Commission from having regard to matters currently before the Court, and prohibits the publication of law enforcement methodology where such information is not already in the public domain. The Commission has been careful to report within those parameters. Further, submissions were called for and received from the QPS in respect of the adverse finding ultimately made.

The hearings were held over five days and the Commission heard evidence from the following witnesses:

1. Mr Ken Gamble – a private investigator
2. Mr X – spokesperson in relation to the 2011 complaints
3. Detective Senior Sergeant Stephen Tiernan – officer of the QPS (formerly of the FCCG)
4. Detective Senior Sergeant Mitchell Castles – officer of the QPS (formerly of the FCCG and currently seconded to the Crime and Corruption Commission)
5. Detective Senior Sergeant Jon Strohfeldt – officer of the QPS (FCCG)
6. Detective Inspector Philip Roach – officer of the NSW police service
7. Detective Superintendent Brian Hay – officer of the QPS (former Detective Superintendent, FCCG)
8. Assistant Commissioner (Retired) Gayle Hogan – retired officer of the QPS (State Crime Command)

The evidence given both in the hearings and by way of further information focused on the issues arising out of the information provided by Detective Superintendent Brian Hay and by Mr Gamble, in particular:

- the nature and extent of the cold-call investment fraud problem on the Gold Coast
- the response of the QPS
- prioritising work and resourcing issues
- the attitude towards complainants.

**Nature and extent of the problem**

As already mentioned, the evidence established that organised crime networks are operating boiler-rooms on the Gold Coast, and have been for a number of years. The schemes are elaborate and sophisticated, fleecing people across Australia of millions of dollars. The former head of the FCCG has described boiler-rooms as ‘criminal call centres’ and agreed that they pose a significant problem.49 The problem was also described as an epidemic and out of control. One senior officer involved in current investigations agreed that the Gold Coast is the hub, with the whole boiler-room industry currently situated in our backyard.50
It was also established that cold-call investment frauds take a number of forms, broadly stated by the QPS as involving either the sale of software for betting or sports arbitrage, or the management of funds. The types of scams promoted by boiler-rooms have been outlined in the section on Investment and financial market fraud, above, and include schemes selling software for investing in the stock market.

Operators go to elaborate lengths to shroud their cold-call investment frauds with a veneer of legitimacy by registering companies with ASIC, and producing sophisticated websites and glossy brochures to promote the scheme, as well as fake websites for industry groups and magazines purporting to have bestowed the company or scheme with awards. The schemes usually involve a multi-jurisdictional structure, operating bank accounts interstate and/or overseas, using false business addresses and ‘virtual’ offices. To further complicate investigations, once a boiler-room has been operating for about 12 months (or until investors start to demand money or question the legitimacy of the scheme) it will often ‘phoenix’ into another corporate structure in an effort to avoid detection.

The Commission accepts that those complexities make investigations of so-called boiler-rooms time-consuming and labour-intensive. The Commission does not accept, however, that the issues are any more complex than those encountered in, for example, large-scale drug trafficking investigations, cold-case murder investigations or online child pornography websites operating in the anonymous environment of the Darknet.

The complexities and typical modus operandi are known to the QPS. Numerous documents demonstrated to the Commission that the ‘life cycle’ of a typical boiler-room is known, as are the common tactics of trickery and the practice of phoenixing. The sham of interstate offices and bank accounts is known, as are the use of ‘dummy’ directors and apparently legitimate corporate structures. It is also well-known that, even in the case of schemes involving the sale of software, cold-call investment frauds use aggressive marketing techniques to sell an investment that is never likely be returned, let alone grow as is falsely promised.

**The response of the QPS**

The QPS maintains that it has ‘responded appropriately in a variety of ways to complaints about boiler-room fraud, including conducting traditional investigations, but also by raising public awareness and undertaking preventative action.’

**Prevention strategies**

A constant theme in the information provided to the Commission was that prevention strategies are of critical importance in tackling the problem of boiler-rooms. There is no doubt that such strategies are important, particularly given the reality of finite police resources.

Crime prevention strategies align with the QPS Strategic Plan, which has, as one of its objectives, ‘(r)educing and preventing the incidence of crime, public disorder and road trauma.’ Crime prevention was the ideal of Sir Robert Peel (who is considered the father of policing and who formalised the concept of a civilian police force in England in 1829). Part of the recommendation of the Fitzgerald Inquiry—that community policing be adopted as the primary policing strategy in Queensland—was that ‘preventative policing strategies are to be an integral part of the normal activities of every police officer’.

To that end, prevention features in QPS mission and vision statements and in relevant strategy documents. Prevention strategies also feature in national and international plans to combat fraud and cybercrime.

It was submitted by the QPS that prevention in the form of increasing public awareness (with reference to Project Synergy and Fiscal the Fraud Fighting Ferret, both discussed in more detail below) is one aspect of a ‘multi-faceted approach to boiler-room fraud’, which also includes investigation and disruption. In defending the allocation of police resources, former State Crime Command Assistant Commissioner, Gayle Hogan, summed up the view shared by a number of her colleagues, in saying that ‘the marketing and the prevention work that we do has been one way of multiplying our resources to be able to try to positively impact and educate potential victims.’

Detective Superintendent Hay told the Commission that the two primary tools used for prevention and reduction of financial crime risk are Project Synergy and media releases. The Commission was informed...
that since 2009, the FCCG has conducted nearly 1,000 media interviews and statements and, during 2014, participated in a regular radio segment called ‘Scamwatch’. According to the QPS, all types of consumer frauds were discussed, including boiler-rooms.

Detective Acting Superintendent Terry Lawrence later told the Commission that the FCCG prevention function includes:

- Project Synergy, involving private and public sector engagement to harden target agencies and individuals against current fraud threats, as well as funding for training and capacity-building for officers—including the area of cybercrime and promoting school-based awareness
- community awareness of current fraud threats through FCCG Detectives delivering presentations to over 12,000 people in 2014 at various community group meetings such as Apex, Probus, Rotary, finance industry groups and government sector groups
- offering external training programs to build capacity for external agencies to undertake fraud investigations
- building victim resilience through the Fraud Victim Support Group
- developing a smart phone application, which will prompt a potential scam victim to answer a series of questions about an ‘investment opportunity’ under consideration, with the objective to divert potential victims away from scams.58

Detective Acting Superintendent Lawrence said that the prevention function is of ‘key importance as the QPS does not have capacity to provide an investigative response to the estimated 320,000 fraud victims’ in Queensland.59 That figure is arrived at by extrapolating figures from an Australian Bureau of Statistics survey conducted in 2010–2011, which suggested that 1.2 million Australians aged 15 years or over were the victim of at least one incident of personal fraud over the 12-month period.

Project Synergy

Project Synergy is a crime-prevention initiative. It is funded by the private sector, and the Commission is aware that some aspects of its management are the subject of an investigation by the CCC. Its stated purpose is:

To build the capability of law enforcement, government, industry and the community to prevent, resist and/or better respond to the threats of identity, financial and cybercrime through events, partnerships, engagement, education, learnings, prevention programs, research, thought leadership and development of creative initiatives.60

In a document prepared by Detective Superintendent Hay, the work done by Project Synergy is listed and summarised below:

- Leave a Legacy Not a Debtp program (in partnership with the Queensland Law Society and Australian Chartered Accountants Association) – although there is no evidence about when this happened
- Establishing the ‘Victims of Fraud Support Group’, now known as the ‘Fraud Support and Recovery Group’
- Developing a mobile phone application to assist would-be investors to avoid scams
- Developing Fiscal the Fraud Fighting Ferret (Fiscal) and associated materials to raise cyber safety awareness in primary school children – a pilot program was delivered to seven schools in 2014 and Fiscal attended the Ekka
- Engaging in partnership programs with Bond University (marketing plan for Fiscal), Griffith University (regarding Fiscal and research into advance-fee fraud, ACORN data and the history of fraud), Sunshine Coast University (research into identity crime) and QUT (submission regarding ACORN data analysis and work on Fiscal games and apps)
- Working with Western Union for the SAFE program (where Western Union placed a prominent warning on the front of its transmission form to warn potential scam victims)
Developing the eBay Online Auction Fraud reporting portal
• Establishing a reporting portal for victims of advance-fee fraud (where the matter is reported to the Nigerian and Ghanan authorities)
• Hosting an International Mass Marketing Fraud Working Group meeting
• Implementing the ‘War Driving Initiative’ in March 2012 – a mass letterbox drop alerted people to the dangers of unsecured Wi-Fi networks (particularly identity crime) and involved police driving around selected areas to identify unsecure networks
• Delivering a training in statement-taking to government and private sector investigators and auditors
• Working with AusCERT (Australian Cyber Emergency Response Team) to host workshops, conferences and working group meetings
• Developing a community program with the Police-Citizens Youth Club
• Presenting at various conferences and symposiums in Australia and overseas
• Hosting the annual Identity, Cyber and Financial Crime Symposium since 2013

Not one of those activities was specifically directed at preventing boiler-room frauds or educating the public as to their existence and modus operandi.

Project Synergy is self-funded by money raised from corporate sponsors, events and training. Detective Superintendent Hay was unable to say how much money is raised annually, except that the conference (also referred to as the symposium) may have raised $60,000, and that anywhere between $15,000 and $45,000 might have been generated by the provision of training.

Project Synergy is managed by the staff of the Fraud Prevention Unit, which sits within the FCCG. That unit is staffed by a senior sergeant (as project manager), a detective sergeant and a plain clothes senior constable (in the role of fraud prevention officer).

The detective sergeant is a trained investigator, who is employed full-time within the prevention unit in a supervisory role. The Commission was told that (as at July 2015) that officer organises the annual symposium, delivers public presentations to community groups, and works on the victim support group by coordinating speakers and attending the monthly meeting. The Commission considers it a misdirection of resources to engage a trained detective, full-time, in the Fraud Prevention Unit.

Until recently (when Detective Terry Lawrence became the Acting Superintendent in the FCCG), the fraud prevention officer performed various functions, including ‘driving’ Project Synergy. That involved providing assistance in determining what direction that project would take and what it aims to achieve. That officer also did a deal of work with the victim support group. The Commission learned that the fraud prevention officer spent 10 months developing the Fiscal campaign and was continuing to work on developing additional modules with the help of the senior sergeant (again, as at July 2015).

Beyond developing further modules for the Fiscal campaign and running the victim support group, it is unclear what work was previously undertaken by the senior sergeant. Detective Acting Superintendent Lawrence told the Commission that the senior sergeant now assists him as well as performing her role in the Fraud Prevention Unit.

It is also unclear how much money has been spent on the Fiscal project which, to date, has not progressed beyond the pilot presentation in seven schools at the end of 2014. In light of the plethora of tools already available to caregivers and educators to further the cyber safety of children, and while the ongoing epidemic of serious and organised financial crime continues, the Commission considers that scant resources should not be further directed to the Fiscal project.

The Commission acknowledges the importance of crime prevention and is cognisant of the impossibility of measuring the impact that past prevention strategies have had. However, it is abundantly clear that efforts to date have been unsuccessful in dealing with the cold-call investment frauds operating on the Gold Coast. In fact, despite the prevention efforts made by the QPS, that type of serious organised crime has flourished, largely unabated.
Investigations

The QPS pointed to three investigations to support the contention that the FCCG has, in general, adequately responded to complaints about boiler-room frauds.\textsuperscript{56} The first investigation—Operation Juliet Dynamite—was conducted in 2011 and 2012. Operation Juliet Dynamite was led by Detective Sergeant Castles from September 2011. That operation was formed as a result of Taskforce Galilee. It was a joint operation undertaken with the ACC and ASIC, and occupied the entire resources of the two major fraud teams. By the time Operation Juliet Dynamite commenced, intelligence work had been done by Taskforce Galilee, so that active investigation commenced immediately, with search warrants executed in December 2011 and arrests made in June 2012. The operation had the assistance of ACC investigators in the early stages, as well as forensic accounting and legal support.\textsuperscript{57} At that time, there were insufficient resources to deal with any other major fraud investigations—including other suspected boiler-rooms—yet it seems that no requests were made for further resources.\textsuperscript{68}

Operation Juliet Dynamite led to the arrest of Carlisle and Crouch (see the case study in the Investment and financial market fraud section earlier in this chapter).

The second investigation mentioned by the QPS involves a matter currently the subject of a judicial proceeding. In accordance with the Terms of Reference, regard is had to that matter only to the extent of examining the progress of the investigation. The Commission draws no conclusions about the strength, or otherwise, of the evidence gathered in the course of it. In fact, the Commission has not seen any such evidence.

The QPS submits that the Commission would find that this matter is an example of the FCCG’s adequate response. However, far from being an example of an adequate response, the matter highlighted serious concerns about inaction and poor prioritisation as outlined below.

After initial investigations (competently and efficiently undertaken, despite few resources and little experience in the area) by Detective Inspector Phil Roche of the NSW Police (with some pro bono assistance by Mr Gamble), the matter was determined to be within the Queensland jurisdiction and a senior officer in the NSW fraud squad determined that it should be transferred to the QPS for further investigation.\textsuperscript{69}

In order to effect the transfer, Detective Inspector Roche made numerous attempts to contact the FCCG, but his calls were left unreturned. When he finally made contact in September 2011, the Detective Inspector Roche was told of short-staffing and workload issues. His impression was that the FCCG was not keen to take on the investigation and that they were very stretched for resources.

Detective Inspector Roche continued to conduct investigations given concerns he held about the matter, and in early 2012, the file was transferred to Queensland. It was only after the ABC ran a 7.30 Report story in September 2012 that the matter was prioritised by the FCCG.\textsuperscript{70} Detective Superintendent Hay said that he does not believe he was aware of the matter prior to the media report.\textsuperscript{71}

The QPS investigation was commenced in September 2012. One investigator was allocated the task. Later, the investigation was assigned to a different officer, who then went on extended sick leave. Detective Inspector Roche gave that officer a brief of evidence in July 2013, and believes that little has been added to it since then. The QPS submit to the contrary.

The Commission does not need to determine who is right about the contribution to the brief of evidence. The fact is that the investigation lay dormant in the FCCG for 18 months while the investigating officer was on sick leave. It was only after Detective Senior Sergeant Tiernan (in his role as Detective Acting Inspector in the FCCG) allocated the investigation to one of the major fraud teams in the latter part of 2014 that the investigation progressed to an arrest in May 2015. During that period, more time was wasted with officers spending a long time reviewing and re-assessing voluminous material in circumstances where there had been no practice of keeping running sheets for investigations.\textsuperscript{72} That is bad practice and, to the extent that it continues, it should be rectified.
Finally, the QPS points to an investigation that has also recently led to arrests as an example of the adequacy of the QPS response to the problem of boiler-rooms operating on the Gold Coast. That investigation was the subject of a joint CCC and QPS investigation commenced in March 2015. Again, in accordance with the restrictions placed on it by the Terms of Reference, the Commission has not had regard to the substance of any matter, and comments made about the progress of the investigation are not intended to impart any view as to the merits of any particular case.

The QPS submits that prior to that joint operation, investigations had commenced in November 2013. That stage of the investigation is said to have been conducted by the FCCG, simultaneously with other boiler-room investigations being undertaken by the FCCG (in its own right and in cooperation with other agencies, including the ACC and the CCC). It is said that the delay in progressing any investigation into the 2011 complaints must be understood in that context.

The Commission does not accept that submission.

Information received by the Commission suggests that the suspected syndicate targeted by the joint operation might have been operating since as far back as 2006. It was initially under investigation by what was then known as the QPS Fraud and Corporate Crime Group (now the FCCG) in 2008 when search warrants were executed. While that measure might have had some disruptive effect on the alleged cold-call investment fraud, the investigation did not progress further.

The suspected syndicate then came to light again during Operation Juliet Dynamite, when intelligence sources suggested ongoing trade.

In late 2014, during another CCC operation, further information came into the hands of the FCCG and was ultimately received by the FCCG. What followed was an agreement that with the resources and the specialist skills that the CCC had at its disposal, the QPS could take the investigation on as a joint partner agency with the CCC. The instrument establishing that operation was signed by the QPS and the CCC in early 2015.

Given the lack of active investigation of that alleged syndicate from 2008 (when the disruption efforts were made) until late 2014/early 2015 (when the joint operation commenced), it could not be said that the resources of the FCCG were stretched by an investigation of this matter during the period of inaction in respect of the 2011 complaints.

The 2011 complaints had been lodged with the QPS from as early as February 2010. Consistent with evidence of confusion on the part of many complainants about where and to whom to lodge a complaint, various local stations received complaints in 2010 and 2011. Ultimately, the FCCG received a detailed report from Mr Gamble in early April 2011. That report contained a great deal of information, including a comprehensive overview of the allegations, yet it was largely ignored by officers in the FCCG. The reasons for that are discussed further below.

The evidence received by the Commission established that between April and September 2011, responsibility for this matter was bounced between the South East Region and the FCCG. Correspondence shows that on 30 September 2011, a request that the matter be referred back to the South East Region (in particular to Gold Coast police) was rejected. The matter has remained dormant in the FCCG since then.

Mr X (the spokesperson for the 2011 complaints) was told in January 2012 that the matter of the 2011 complaints was to be assessed by the FCCG, and by 12 January 2012 that the case had been assessed. Having been told that the case had been assessed, Mr X was also informed that the matter would remain with the FCCG but that no detective had yet been assigned to investigate it.

The Commission was told that in order to assess first, whether a matter (including the 2011 complaints) is civil or criminal, and second, to determine the appropriate allocation of resources according to priority, the Case Assessment Unit within the FCCG undertakes an assessment. The Commission sought the Case Assessment Unit assessment of the 2011 complaints, but aside from an assessment of one related complaint made in 2010, none was provided. The only conclusion available is that, aside from in that particular case, no assessment was made, despite what Mr X had been told.
Certainly, it was made very clear to Mr X that regardless of a favourable assessment (in the sense of assessing it as an appropriate matter for investigation by the QPS), the 2011 complaints were not a high priority, because they were not considered to relate to current offending.78

As to the nature of the alleged offending, there is no evidence to suggest that the FCCG followed any of the leads provided to them in Mr Gamble’s report, not even to establish if the alleged criminal syndicate continued to operate in a ‘phoenixed’ form. In fact, in late 2012, Detective Superintendent Hay delegated that task to the complainant, saying that if he could show evidence of current offending, it would ‘make it a priority job as opposed to a job on wait, on hold.’79

The problem of scant resources was compounded in this case by the attitude taken by the then-Detective Superintendent Hay and Detective Inspector Strohfeldt to the information provided by Mr Gamble and, in some respects, towards the complainants.

Mr X told the Commission that he perceived both officers to be ‘anti-Ken Gamble.’ He recalled Detective Inspector Strohfeldt suggesting that Mr Gamble (and by inference his report) would be biased toward what his clients wanted to hear, and telling MR X that any investigation undertaken by Gamble would have to be repeated by the QPS.

Detective Superintendent Hay told the Commission that then-Detective Inspector Strohfeldt described Mr Gamble’s report as ‘a heap of crap’.80 Detective Inspector Strohfeldt does not recall using those words, however he did think the report was a waste of money and of ‘no evidentiary value whatsoever.’80

Clearly, neither Detective Superintendent Hay nor Detective Inspector Strohfeldt shared the view of a number of other senior investigators that Mr Gamble’s report was, at least, a high-level intelligence product. It is difficult to understand how Detective Superintendent Hay formed that view since it was conceded in evidence that he had not read the report.82

Whereas the investigators at the CCC, the head of the NSW Fraud Squad and a senior regional officer—as well as other officers in the QPS—had found Mr Gamble to be a helpful resource, the FCCG (or at least its most senior officers) viewed him and his product as self-serving. That was misguided and a wasted opportunity.

Detective Superintendent Hay saw ‘the Ken Gambles of the world…as a personal battle’, perceiving him to be making promises to his clients that he expected the QPS to deliver on. Detective Superintendent Hay was also angered by the use of the media and complaints to politicians about police inaction. That frustrated him, since ‘we still had our priority issues to address.’83 Detective Superintendent Hay, and others in the FCCG, felt that they were being manipulated to prioritise the investigation of this matter over others.

The evidence was to the contrary. Mr X presented as exasperated but reasonable. He realised from the beginning that the report compiled by Mr Gamble would not be sufficient to effect the arrest of alleged perpetrators, and he expected that further investigation by the police would be required. Mr X understood that there may be issues regarding whether the complaints warranted criminal investigation, and he was trying to understand whether his case (and those of the others he spoke for) would qualify.

Detective Superintendent Hay met with Mr X on one occasion84 in late 2012, and suggested that he and other complainants involve themselves in the FCCG prevention strategies by appearing in the media to warn others of investment scams. By that time, Mr X (who initially thought that might be a positive step), and the group of complainants he spoke for, were disillusioned by the lack of response by the FCCG to their complaints and were dubious about the value of what had been suggested. Mr X said his group thought this was ‘just a way of shutting us up again.’85

In 2014, with no progress having been made, Sergeant Tiernan asked Detective Superintendent Hay how he should allocate the dormant 2011 complaints. He was told to allocate them to the ‘boiler-room taskforce’. No such task force existed then, nor does it exist now. Detective Superintendent Hay knew that no task force existed but explained, unconvincingly in the Commission’s view, that it was not his intention that the matter remain on stand-by for a further, undetermined period awaiting the establishment of a boiler-room task force, but that there were plenty of things that could be done to prepare for a future investigation in that time.86

Certainly nothing had been done until after the Commission’s hearings in July 2015.
The Commission is told that since the hearings, Sergeant Tiernan has returned to the FCCG and has met with Mr X. The 2011 complaints have been allocated to an investigator within the FCCG.

The Commission was further comforted by information provided by Detective Acting Superintendent Lawrence after hearings had concluded, and in submissions made by the QPS. It is evident that work is being done to address some apparently active boiler-rooms and to progress other matters that have languished without appropriate action.

Finally, during the course of the Inquiry, a Memorandum of Understanding was reached between Deputy Commissioner Ross Barnett and the Commissioner of the Inquiry, Michael Byrne QC, regarding the handling of fresh complaints that had been made directly to the Commission of Inquiry from members of the public. That was a positive step towards improving the way that the QPS responds to complaints of that nature.

**Resources and prioritisation**

There are two Major Fraud Investigation Units within the FCCG.

As alluded to earlier, the Case Assessment Unit determines prima facie whether a matter is one for criminal investigation or whether it is a civil matter. The Case Evaluation Committee makes determination when there are more complex matters to consider in respect of whether a matter is to be investigated by the FCCG.

The allocation of matters for investigation is made by the Detective Superintendent or the Detective Inspector. The Operational Procedures Manual prescribes the ‘terms of engagement’ for the FCCG.

One of the reasons why some complaints made to the QPS are not investigated is that they are assessed as being civil rather than criminal matters. Alternatively, even where there is some suggestion of criminal conduct, the finite resources of the QPS mean that complainants have been referred to other regulatory authorities that are perceived to be ‘better positioned to take management’ of the matter.87

The categorisation of an alleged fraud as a criminal matter is the threshold test for the QPS in deciding if it will be investigated. That is quite proper, and one way of allocating resources appropriately. It became apparent, however, that there is significant confusion as to the proper test to be applied both legally and procedurally.

The confusion seems to be prevalent in considering alleged boiler-room frauds involving the sale of a product, usually software. Detective Superintendent Hay said that he draws a distinction in respect of a person who receives the product that they had paid for under a contract, which also provides no guarantee as to outcome (despite what the person might be told over the telephone). That is a case, according to Detective Superintendent Hay, that might properly be for investigation by the Office of Fair Trading (rather than the QPS).88 Further, while agreeing that the fact that a person received a product is not determinative of the question of criminality, Detective Superintendent Hay did say that that fact is relevant to the priority a matter will be given.

It is very concerning that the long-time head of the FCCG holds those views, despite the cornucopia of information and intelligence supporting a conclusion, in many cases, that the software-selling scheme is, in fact, organised crime.

Confusion among the ranks is also evident. At a three-day Fraud Squad Regional Workshop conducted in May 2015, the planned program of workshops and education in respect of a range of topics (covering a number of financial crime types, investigation methods and brief preparation) gave way to this issue. The Commission was told that the workshop focussed heavily on the legal meaning of the words in section 408C (Fraud) of the Criminal Code, as well as the legal meaning of dishonesty and what distinguishes a criminal matter from a civil dispute.89

The process of assessing whether a matter is criminal or civil is performed by the Case Assessment Unit or the Case Evaluation Unit within the FCCG. Outside of the FCCG, police officers with varying degrees of expertise in this area no doubt make decisions as to the merits of a complaint from time to time. It is, therefore, important that the correct legal test and other relevant criteria is applied and, importantly, that the test and criteria are only applied once there is sufficient information to render the result meaningful.
Dishonesty

The legal meaning of dishonesty, for the purpose of proving fraud, confuses many lawyers, so it is understandable that police officers sometimes grapple with the application of the law to the facts of fraud complaints. The Commission gained some insight into the interpretation of the law relating to dishonesty in the information provided by the Detective Acting Superintendent of the FCCG. That information also disclosed particular aspects of typical boiler-room operations that are said to make the element of dishonesty difficult to prove to the criminal standard.

The Court of Appeal recently considered, in R v Dillon; Ex parte Attorney-General (Qld), what must be proved to satisfy the element of dishonesty in section 408C Criminal Code. That decision was delivered in response to a reference by the Attorney-General under section 668A of the Criminal Code on a point of law, namely:

To satisfy the element of dishonesty does the Crown have to prove that:

1. What the accused person did was dishonest by the standards of ordinary honest people; and
2. The accused person must have realized that what he or she was doing was dishonest by those standards?

The answer to the question was no. The Court held that the term ‘dishonestly’ in section 408C requires the prosecution to prove only that what the accused person did was dishonest by the standards of ordinary honest people. In other words, it was not necessary to prove that the accused person realised that what they were doing was dishonest by those standards.

That represents a departure from the previously settled approach in Queensland, which was to apply the two-tiered test for dishonesty espoused in the English case of R v Ghosh and mirrored in section 130.3 (Meaning of dishonest) of the Criminal Code (Cth). The test now to be applied accords with the High Court decisions in Peters v The Queen and Macleod v The Queen. That change ought to dispel much of the existing confusion and the concern about the evidentiary challenges of proving a person’s state of mind.

Sufficiency of the evidence and public interest tests

Police officers assessing the nature of a complaint (and therefore whether it might be investigated) are instructed to take into account factors relating to the sufficiency of the evidence, and the public interest. Those factors are articulated in section 3.4.3 (‘Factors to consider when deciding to prosecute’) of the QPS Operational Procedures Manual (QPS Manual).

Chapter 3 (‘Prosecution Process’) of the QPS Manual, however, expressly provides that the provisions contained within it only come into effect after an offender is identified through the investigative process. The procedures relevant to that process are set out in Chapter 2 (‘Investigative Process’).

To have regard to the sufficiency of the evidence and the public interest in order to determine if an investigation will take place—or what priority it will be given—is to put the cart before the horse. The practice should stop. It is very likely to result in wrong determinations being made about the nature of the complaint (as criminal or civil) because there is too little, if any, evidence to make any sound assessment of the prospects of ultimately proving a charge against an offender. In fact, without at least some preliminary investigation, it is sometimes not possible to know even the identity of the offender(s).

As to the application of the public interest test, it is hard to imagine a case involving a boiler-room that would not pass the test. Again, however, the relevant factors set out in section 3.4.2 of Chapter 3 of the QPS Manual cannot be properly considered with the scant information or evidence available before an investigation has commenced. By way of stark example, it is impossible to consider the following factors (relevant to the assessment of public interest) before an investigation has commenced:
5.12 The Commission recommends that the Queensland Police Service ensure by appropriate means that all operational police officers are aware that:

- It is not appropriate to have reference to section 3.4.3 (Factors to consider when deciding to prosecute) of the Queensland Police Service Operational Procedures Manual when assessing whether a complainant is civil or criminal in nature; in determining whether it will be investigated by the Queensland Police Service, and if so, what priority it is to be given.

- The law relating to the element of dishonesty in section 408C of the Criminal Code has changed by virtue of the decision in R v Dillon; Ex parte Attorney-General (Qld) [2015] QCA 155.

FCCG priorities

Once it is determined that a matter is properly a matter for police response, it is accepted that the QPS must prioritise work in order to appropriately allocate finite resources to infinite demand. It is also accepted that priority must be given to matters of public safety and the protection of human life. In the current structure of the State Crime Command, all groups but the FCCG have an obvious public safety aspect.

Detective Superintendent Hay said that there had been a backlog of work throughout his entire 12 years in charge of the fraud squad. When he first arrived at the post, there was a depository for files awaiting allocation for investigation known as the ‘cupboard of death’. The Commission also saw reference to the ‘black hole’ in the fraud squad. Whatever the term used, there is clearly a long-standing resourcing issue in the FCCG.

That issue is exacerbated from time to time by the reassignment of human resources out of the fraud squad to deal with matters deemed to be of higher priority. Past examples include the secondment of officers to assist in the police response to serious flood events in Queensland, and, more recently, more than 20 officers from the FCCG have been allocated to work in Taskforce Maxima.

Some of the officers allocated to Taskforce Maxima are currently involved in the investigation of suspected boiler-room frauds at the CCC. Those investigations came out of investigations into outlaw motorcycle group members and suspected links to boiler-room frauds on the Gold Coast. Further, from time to time, the FCCG has been instructed by ‘senior management’ to prioritise certain matters—including alleged frauds on the government. Such matters have included the so-called ‘Tahitian prince’, Joel Barlow, and a matter involving Q-Build. The Commission was told that the prioritisation of matters involving the government is usually determined ‘higher up’, but not unjustifiably, according to a senior officer who pointed out the significant loss to the taxpayer as a result of Barlow’s fraud on Queensland Health. It could hardly be said, however, that that fraud was ongoing or presented a risk to public safety.

Similarly, during the period when the 2011 complaints sat unallocated and another matter uninvestigated, the Commission was told that an investigation involving a private matter between husband and wife, or bank and mortgagor, took priority over the investigation of the alleged boiler-room frauds. That seems a nonsensical allocation of resources.
Attitude to complainants

A number of QPS officers expressed frustration that complainants in boiler-room fraud matters had not exercised due diligence. Both a former and a current Assistant Commissioner stated that it was their individual view (expressed by each in almost identical terms) that:

[A] common and consistent theme remains with a majority of fraud and related offences:

- Complainants/Victims fail to exercise even very basic due diligence before committing tens or hundreds of thousands of dollars;
- Returns often expected by complainants/victims were unrealistic when considering the financial environment at the time and returns offered elsewhere;
- [There] seemed a general expectation on the QPS to deal with a fraudulent financial disaster which could have been avoided if regulatory agencies had intervened to stop the offer of a financial product without an Australian Financial Service’s [sic] licence, or issue embargo notices to prevent the supply of fraudulent financial services;
- Industry needs to take greater responsibility and diligence when marketing their investment products;
- Despite constant warnings and recommendations a limited number of complainants/victims seek independent advice on investments; and
- In some instances complainants/victims utilise free police resources as an alternative to costly civil action.98

In addition to that shared view, Assistant Commissioner Condon stated that:

All of these complainants/victims actions continue to impact on police resources. The Queensland Police Service and I suspect other law enforcement agencies across the nation cannot arrest their way out of this growing problem. There is a requirement for the community to take responsibility for their own actions and to exercise a higher level of care and diligence as criminals become more savvy in exploiting the vulnerable.99

Those assumptions and beliefs about the victims of financial crime are no doubt shared by other officers tasked with dealing with complaints and allocating resources.

The QPS submitted that the evidence before the Commission does not support a finding that an inadequate response to complainants about boiler-rooms is attributable in part to the attitude that complainants do not exercise due diligence concerning their finances. It submits that, at its highest, the attitude is the manifestation of frustration that preventative measures, such as exercising due diligence, were not being effectively undertaken by complainants.100

That frustration—and the attitude it has engendered—is misplaced in the case of many victims of boiler-room frauds. It is at odds with the evidence repeatedly given by QPS officers about the sophistication of boiler-room operations. As already mentioned, the tactics of those operations to create a veneer of legitimacy are well-known to police, including the use of convincing advertising material and apparently legitimate business structures to avoid the suspicion of investors who undertake due diligence checks with ASIC. It is unacceptable to cite the complexity of the operations as part of the policing dilemma on the one hand, and express frustration that victims are falling prey to them on the other.

It is accepted that there is no direct evidence of attitudes and beliefs about victim responsibility directly affecting the conduct of investigations, the allocation of resources to boiler-room investigations, or the priority given to those investigations. However, there is a wealth of literature that supports a conclusion that organisational culture affects the way people in organisations interact with each other, with clients (the complainants in this case), and with stakeholders.
Here, entrenched attitudes and beliefs held by those in senior leadership roles are bound to filter down and influence the way officers approach complaints of this nature, consciously or otherwise. A cultural change is needed to address unfair allocation of blame—or shifting of responsibility—to victims of serious and sophisticated organised crime.

**Finding**

The Commission finds that the Queensland Police Service has failed to adequately respond to complaints from persons claiming to have been defrauded by people operating boiler-room schemes. This failure is largely attributable to inadequate resourcing and likely influenced by an attitude that the complainants have failed to exercise diligence concerning their own finances.

**Solutions**

**A boiler-room task force**

In the context of reiterating that the State Crime Command continues to focus on those matters with the greatest risk, Assistant Commissioner Hogan stated that ‘(d)ue to limited resources [State Crime Command] has set up a Task Force with a number of other state and federal agencies utilising state and federal legislation to attempt to interdict those currently offending.’\(^\text{101}\) No such task force has in fact been established.

Detective Superintendent Hay has been agitating for the formation of a multi-disciplinary boiler-room task force for some time. His plan was to involve other agencies and industries in the task force in an effort to disrupt boiler-rooms, thereby obviating the need for protracted investigations and saving more people from loss. In Detective Superintendent Hay’s view, investigative solutions to organised crime are redundant.\(^\text{102}\)

In May 2015, officers of the FCCG arranged a meeting of representatives of the Office of State Revenue, the ATO, the ACC, the CCC and regional QPS officers. A presentation of an intelligence report (from January 2015) was given. Sometime later, a meeting was held with stakeholders with a view to forming agreements about contributions to such a task force.

Nothing came of those meetings.

A potential solution to part of the resourcing problem was suggested by the Commission. Since fraud investigations are always likely to take the lowest priority in the State Crime Command where public safety understandably comes first in the allocation of resources, it was suggested that consideration be given to removing the FCCG from State Crime Command. The rationale behind that suggestion is that the FCCG might then be quarantined from the loss of resources to matters of higher priority.

That suggestion was not supported by the QPS, nor was it accepted that FCCG holds the lowest priority in terms of resources within State Crime Command.\(^\text{103}\) In apparent contradiction to the latter proposition, the QPS said that it has consistently prioritised investigations and the allocation of resources to identifiable threats to the Queensland community by reference to the following criteria:\(^\text{104}\)

- public safety—more specifically, risk of physical harm
- public interest
- directions from executive government.

Further, the QPS emphasised the importance of maintaining flexibility to respond effectively to high-priority, emerging or urgent threats affecting public safety and legitimate areas of community concern.\(^\text{105}\)

The Commission was repeatedly told that the allocation of resources across the command is a balancing act that must take account of the matters above, as well as obligations under the *Police Service Administration Act 1990* and the *Police Service Administration Regulation 1990*, strategic priorities and objectives, and
the public interest (involving ‘identification of the highest threat to the community in line with community expectations’).106

Of course, public safety must always take priority where allocation of resources is concerned; however, it is a function of the QPS under the Police Service Administration Act to detect offenders and bring them to justice, to prevent crime, and to uphold the law generally.107 It is in the public interest that this function be fulfilled in respect of boiler-room frauds. They are a type of organised crime, and they continue to cause significant financial loss and other serious consequences to people in Queensland, as well as to people in other parts of the country and overseas.

To that end, the QPS, whether within State Crime Command or elsewhere in the service, must be properly resourced to address this organised crime threat. The FCCG has not had sufficient resources in the past, and that has been made worse by the diversion of a significant number to investigating outlaw motorcycle groups which, members of which account for only 0.52 per cent of persons charged with criminal offences in Queensland over the last 21 months.

The QPS submits that:

[W]hile greater resourcing would enhance the QPS’s capability to respond to unlawful boiler-room operations...other factors also have a significant impact on the QPS’s capability to effectively respond to these threats, including:

• The complexity of the schemes, which involve multiple people;
• The difficulty in distinguishing between civil and criminal matters at least in the early stage of investigation;
• The capacity of boiler-room operations to shut down quickly and the likelihood that victims may not complain until after an operation has shut down;
• The specialist skills and time required to successfully bring a matter to prosecution;
• The cross-jurisdictional nature of the many of the investigations.108

For those reasons, the QPS contends that ‘resourcing alone does not address the many challenges faced when investigating the activities of unlawful boiler-rooms’ and that simply applying further resources to the investigation of such schemes will not necessarily address the issue.109

The Commission does not accept that the complexities of boiler-room frauds render them beyond the capability of the QPS to effectively address (whether by early disruption or investigation). Proper resourcing of a dedicated unit or task force, including with people with the requisite specialist skills, would go a long way towards addressing this serious organised crime problem. Rather, the Commission agrees with the statement made by Acting Detective Superintendent Lawrence that ‘(c)ombating CCI fraud in Queensland in the immediate future requires substantial resourcing and collaboration directed toward both investigation and regulatory disruption.’110

Acting Detective Superintendent Lawrence has provided the Commission with a detailed proposal for the structure and resourcing requirements of a boiler-room task force should one be established. His proposal is that a QPS investigative team should include a number of QPS investigators, forensic accountants and intelligence analysts, as well as access to covert strategies.111

As to the operation of such a task force, Acting Detective Superintendent Lawrence suggests:

The investigative team should operate in collaboration under a standing arrangement with at least the Office of Fair Trading (OFT), the Office of Liquor Gaming Regulation (OLGR) and CCC through a standing reference for CCO fraud. The OFT has powers to enter business premises, inspect records and to order a business to stop trading under threat of prosecution. The OLGR has powers for enforcing gaming machine and wagering laws, including with respect to employees. The CCC has significant powers to conduct coercive hearing for intelligence purposes, and resources for covert strategies.
The Australian Securities and Investments Commission (ASIC) and the Australian Taxation Office (ATO) should also have a standing collaborative role. ATO action to enforce GST remittance, undertake taxation assessments on the relevant companies, operators and employees is likely to help drive participants from the industry and force the closure of corporations and their bank accounts. The systematic removal of funds from CCI fraud company bank accounts is essentially taking company assets and rendering it insolvent. ASIC has powers to conduct examinations, force the return of funds, ban individuals as company directors and to seek the appointment of liquidators with a view to winding up and de-registering relevant companies. Again, such action prevents a CCI fraud from operating.

Other federal agencies such as Australian Border Force could have a role in dealing with CCI fraud employees who are visa ‘overstayers’ or who are working contrary to tourist or student visa. Similarly, Centrelink could have a role in dealing with CCI fraud operators or employees who receive income while also receiving social security benefits.

An initial joint QPS, OFT, OLGR, CCC, ASIC, ATO and Centrelink response each using their respective investigative or regulatory powers could efficiently remove CCI fraud operator’s capacity to commit crime.112

It is noted that one of the ‘enhanced response activities’ suggested by the National Organised Crime Response Plan 2015–2018 is the establishment of a multi-agency Serious Financial Crime Taskforce within the Fraud and Anti-Corruption Centre. That task force is to ‘provide a practical Commonwealth response to high priority serious financial crime, informed by the ACC Financial Crime Risk Assessments.’ Further, under the Plan, ‘the Commonwealth will explore options to share lessons learned with states and territories.’113 The QPS might take advantage of that national initiative (and any resources it might offer to addressing onshore CCIF) through its involvement in the Queensland Joint Analyst Group.

### Recommendation

#### 5.13

The Commission recommends that the Queensland Police Service establish a dedicated taskforce, resourced by specialist investigators and other personnel, to address cold-call investment frauds.

### Training

The Commission shares the view expressed by Detective Superintendent Hay that QPS staff must be properly trained to deal with fraud and cybercrime. A draft curriculum for a proposed training course relevant to economic crime has been developed. The proposal includes training in boiler-room strategies, and education in the legal and regulatory framework.114 It is envisaged that the course would be delivered to new recruits.

### Recommendation

#### 5.14

The Commission recommends that the Queensland Police Service include the economic crime course in the curriculum for new recruits and for detective training. A refresher course should be developed and implemented for existing detectives.
5.6.2 Crime and Corruption Commission

As previously indicated, the CCC investigates matters referred to it by the Crime Reference Committee. Currently, there are general referrals relating to six areas of major crime, including organised crime and money laundering.\(^{115}\)

Before the CCC can become involved in an investigation (either on its own or as a member of a joint agency task force) it must be demonstrated that the unique powers of the CCC and its specialist staff are required to achieve successful operational outcomes.

The Commission has been made aware of recent submissions regarding the Crime Reference Committee and its referrals, made by the CCC to the Parliamentary Crime and Corruption Committee review of the CCC. These submissions and the related recommendations aim to clarify ambiguities, remove unnecessary distinctions and allow time-sensitive matters to be responded to more efficiently.\(^{116}\)

The CCC has a dedicated organised crime multi-disciplinary investigative team comprising investigators, intelligence analysts, lawyers, financial investigators, physical and technical surveillance specialists and computer forensic analysts. This team has both the time, skills and available resources to undertake complex and long term investigations.

Until 2014, the CCC had limited involvement in the investigation of organised financial crime. Its foray into this area commenced when it held hearings in support of a QPS investigation.\(^{117}\)

As Queensland law enforcement developed a better understanding of boiler-room fraud, its complexity and the volume of resources required to investigate it, the CCC agreed to undertake at least two investigations into alleged boiler-room fraud on the Gold Coast, and has formed a special investigations unit for that purpose.\(^{118}\) It should be noted that the QPS continues to contribute substantial human resources to the task forces and pays their salary from the QPS budget.\(^{119}\)

The CCC also has a function in the recovery of the proceeds of crime pursuant to the *Criminal Proceeds Confiscation Act 2002* (Qld) and the significant power to compel witnesses to give evidence in coercive hearing.

5.6.3 The Queensland Office of the Director of Public Prosecutions

As set out the chapter on outlaw motorcycle gangs, the role of the Queensland Office of the Director of Public Prosecutions (ODPP) is to prosecute offenders on behalf of the State of Queensland, and in certain circumstances to assist victims and apply for the restraint or confiscation of proceeds of crime. There is nothing to suggest that the ODPP responds other than appropriately to organised financial crime.

It has also been said that the ODPP does not collaborate with the QPS during an investigation in the same way equivalent agencies interact in the United States. There is scope for such collaboration, although it is rarely engaged.

Given what the Commission has learned about the difficulties experienced by QPS officers in determining threshold issues in relation to fraud (for example, as to whether a matter is civil or criminal), some assistance from the ODPP may be warranted.

**Recommendation**

5.15 The Commission recommends that the Office of the Director of Public Prosecutions and the Queensland Police Service develop a mechanism for collaboration between the two agencies in respect of assessing alleged frauds for criminality.
(Endnotes)

1 Submission of Queensland Police Service, 22 May 2015, p. 16.

2 Submission of Queensland Police Service, 22 May 2015, p. 16.

3 Submission of Queensland Police Service, 22 May 2015, p. 16.


12 Transcript of hearing, Gayle Hogan, 28 July 2015, line 35, p. 278.


16 Submission of Queensland Police Service, 22 May 2015, p. 22.


18 Statutory Declaration of Terry Lawrence, 20 August 2015, paras 8–18.

19 R v Hennessey (Unreported, District Court of Queensland, Robertson DCJ, 7 July 2014).

20 Statutory Declaration of Terry Lawrence, 20 August 2015, paras 37–41 (claim of confidentiality).

21 Statutory Declaration of Terry Lawrence, 20 August 2015, para 46.

22 FAJ [2013] QCAT 703.

23 Statutory Declaration of Terry Lawrence, 20 August 2015, para 49.


29 Submission of the Queensland Police Service, 2 September 2015, para 21.


31 Transcript of interview, Brian Hay, 19 June 2015, p. 8

32 Transcript of interview, Brian Hay, 19 June 2015, p. 10.

33 Transcript of interview, Brian Hay, 19 June 2015, p. 12.

34 Transcript of interview, Brian Hay, 19 June 2015, p. 23.

35 Transcript of interview, Brian Hay, 19 June 2015, p. 29 (the Commission was not authorised by the QPS to publish the number of investigators).


37 Transcript of interview, Brian Hay, 19 June 2015, p. 9.

38 Transcript of interview, Brian Hay, 19 June 2015, p. 9.


40 Transcript of interview, Brian Hay, 19 June 2015, p. 29 (the Commission was not authorised by the QPS to publish the number of investigators).

<table>
<thead>
<tr>
<th>42</th>
<th>Transcript of interview, Brian Hay, 19 June 2015, p. 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>Transcript of interview, Brian Hay, 19 June 2015, p. 15.</td>
</tr>
<tr>
<td>45</td>
<td>Transcript of interview, Brian Hay, 19 June 2015, p. 23.</td>
</tr>
<tr>
<td>47</td>
<td>Transcript of interview, Brian Hay, 19 June 2015, p. 20.</td>
</tr>
<tr>
<td>49</td>
<td>Transcript of hearing, Brian Hay, 21 July 2015, line 45, p. 145.</td>
</tr>
<tr>
<td>50</td>
<td>Transcript of hearing, Mitch Castles, 20 July 2015, p. 113.</td>
</tr>
<tr>
<td>51</td>
<td>Statutory Declaration of Terry Lawrence, 28 August 2015, para 21.</td>
</tr>
<tr>
<td>52</td>
<td>Using shell companies that have existed for some time.</td>
</tr>
<tr>
<td>54</td>
<td>Submission of Queensland Police Service, 2 September 2015, para 25 [relying on Statutory Declaration of Terry Lawrence, 28 August 2015, paras 17–18].</td>
</tr>
<tr>
<td>57</td>
<td>Statutory Declaration of Brian Hay, 7 July 2015, para 3.</td>
</tr>
<tr>
<td>58</td>
<td>Statutory Declaration of Terry Lawrence, 28 August 2015, para 17.</td>
</tr>
<tr>
<td>59</td>
<td>Statutory Declaration of Terry Lawrence, 28 August 2015, para 18.</td>
</tr>
<tr>
<td>60</td>
<td>Statutory Declaration of Brian Hay, 7 July 2015, Annexure A.</td>
</tr>
<tr>
<td>61</td>
<td>Statutory Declaration of Brian Hay, 7 July 2015, Annexure A.</td>
</tr>
<tr>
<td>64</td>
<td>Transcript of hearing, Brian Hay, 27 July 2015, pp. 185–187.</td>
</tr>
<tr>
<td>65</td>
<td>Transcript of interview, Terry Lawrence, 8 September 2015, p. 38.</td>
</tr>
<tr>
<td>67</td>
<td>Transcript of hearing, Mitch Castles, 20 July 2015, pp. 103–104.</td>
</tr>
<tr>
<td>68</td>
<td>Transcript of hearing, Mitch Castles, 20 July 2015, p. 103.</td>
</tr>
<tr>
<td>70</td>
<td>Transcript of hearing, Phillip Roach, 21 July 2015, p. 130.</td>
</tr>
<tr>
<td>72</td>
<td>Transcript of hearing, Steven Tiernan, 20 July 2015, p. 96.</td>
</tr>
<tr>
<td>76</td>
<td>Transcript of hearing, Mitch Castles, 20 July 2015, lines 3–8, p. 110.</td>
</tr>
<tr>
<td>77</td>
<td>Transcript of hearing, Mr X, 20 July 2015, pp.53, 55 and 56.</td>
</tr>
<tr>
<td>78</td>
<td>Transcript, Mr X, 20 July 2015, p.57.</td>
</tr>
<tr>
<td>80</td>
<td>Transcript of hearing, Brian Hay, 21 July 2015, line 40, p. 162.</td>
</tr>
<tr>
<td>81</td>
<td>Transcript of hearing, Jon Strohfeldt, p.252.</td>
</tr>
<tr>
<td>82</td>
<td>Transcript of hearing, Brian Hay, 21 July 2015, line 7, p. 163.</td>
</tr>
<tr>
<td>84</td>
<td>Mr X thought he met with Detective Superintendent Hay (with Jon Strohfeldt) on two occasions, however cross-examination of both men suggested that Detective Superintendent Hay was correct in recalling only one meeting.</td>
</tr>
<tr>
<td>85</td>
<td>Transcript of hearing, Mr X, 20 July 2015, p.65.</td>
</tr>
</tbody>
</table>
86 Transcript of hearings, Brian Hay, 27 July 2015, p. 199.
87 Transcript of hearing, Brian Hay, 21 July 2015, line 20, p. 147.
89 Statutory Declaration of Brian Hay, 7 July 2015, para 30 & Annexure H.
91 R v Dillion Ex parte Attorney-General (Qld) [2015] QCA 155 at [4].
96 Transcript of hearing, Jon Strohfeldt, 27 July 2015, p. 245.
100 Submission of Queensland Police Service, 2 September 2015, paras 40, 47.
102 Transcript of interview, Brian Hay, 19 June 2015.
103 Submission of Queensland Police Service, 2 September 2015, para 7.
104 Submission of Queensland Police Service, 2 September 2015, para 11.
105 Submission of Queensland Police Service, 2 September 2015, para 12.
107 Sections 2.3(c), (d) & (e) Police Service Administration Act 1990 (Qld).
110 Statutory Declaration of Terry Lawrence, 28 August 2015, para 43.
111 Statutory Declaration of Terry Lawrence, 28 August 2015, para 44.
112 Statutory Declaration of Terry Lawrence, 28 August 2015, paras 45–48.
114 Statutory Declaration of Brian Hay, 7 July 2015, Annexure G.
115 Statutory Declaration of Brian Hay, 7 July 2015, p. 4.
116 A J MacSporran QC, Chairman, Crime and Corruption Commission letter to L Shephard, Executive Director, OCCOI, 13 October 2015, annexing extract of supplementary submissions of the CC to the Parliamentary Crime and Corruption Committee’s review of the CCC (regarding the CCC’s referral system and operation of the Crime Reference Committee).
118 Statutory Declaration of Brian Hay, 7 July 2015, p. 22.
119 Transcript of interview, Terry Lawrence, 8 September 2015.

Queensland Organised Crime Commission of Inquiry 485
5.7 Future trends and emerging markets

5.7.1 Cold-call investment fraud

While boiler-rooms are by no means a new phenomenon, such operations have evolved over time, becoming more sophisticated and presenting a local organised crime challenge for law enforcement agencies.

Since 2011, Taskforce Galilee—led by the Australian Crime Commission (ACC)—has been working to disrupt serious online investment fraud facilitated by offshore boiler-rooms, primarily in Asia. The Taskforce consists of 25 industry organisations and 19 state, territory and Commonwealth agencies, including the Queensland Police Service (QPS).

It is now abundantly clear that boiler-rooms are no longer just an offshore problem. As already discussed, the Commission received much information and evidence to support the conclusion that those types of frauds are rife on the Gold Coast.

As to the mode of offending, traditional boiler-rooms, in their simplest form, involve a fairly straightforward money-in, money-out fraud. For instance, an offender would contact a victim purporting to be a stock broker. The offender would then invite the victim to invest a sum of money, promising a large return on investment. In reality, the victim would transfer money into the offender’s bank account, which would then be transferred out again.

Contemporary boiler-rooms often operate differently, with layers of complexity designed to give the impression of legitimacy. For example, instead of traditional ‘money in, money out’ operations, contemporary offenders may pose as sales people, offering software that purports to predict the stock market or horse racing wins. Victims will often sign formal sales contracts containing a fine-print clause that the program does not guarantee a great yield or return. Further, the receipt of a tangible item (a software package, and, in some cases, a laptop) muddies the waters in determining whether losses are properly the subject of a criminal prosecution, or, rather, a civil dispute.

As mentioned earlier, boiler-rooms also exploit legitimate business structures in order to defeat due diligence efforts made by potential victims (for example, by searching the Australian Securities and Investments Commission website). Boiler-room operations also use marketing tools to their advantage, creating fake brochures and websites to extoll their bona fides and successes.

Like in other areas of organised crime, syndicates operating lucrative boiler-rooms will continue to take advantage of new technologies in efforts to attract victims and to defeat detection and prosecution.

5.7.2 Cybercrime

Interpol notes that new trends in cybercrime are emerging all the time, with costs to the global economy running into the billions of dollars. Further, as to the evolution of cybercrime:

In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing criminal organisations working with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. Highly complex, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organisations are turning increasingly to the Internet to facilitate their activities and maximise their profit in the shortest time. The crimes themselves are not necessarily new (such as theft and fraud) but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

The 2015 Threat Report by the Australian Cyber Security Centre identifies a number of cyber-threats relevant to Australia. Some of these, such as cyber espionage and hacktivism, are politically motivated and are not
generally carried out for financial purposes. Financially motivated cybercrime, however, has been identified as an issue that has flourished in Australia due to the nation’s wealth, high use of technology, and under-reporting of offences to authorities.4

A 2013 industry estimate suggested that the cost of cybercrime in Australia over the previous 12 months was over $1 billion.5 That estimate was based only on self-reported experiences of individuals, and did not include costs to businesses or government agencies. While the Australian Cyber Security Centre encourages the private sector to report cyber breaches, it understands that businesses are often reluctant to do so, given the risk to reputation.

Cybercrime was reported by financial services respondents to the 2012 PwC Global Economic Crime Survey as ‘the second most common type of economic crime after asset misappropriation.’6 The report observed that, despite statistics demonstrating the threat of cybercrime, many financial service respondents act reactively, rather than proactively, to managing cybercrime.7

5.7.3 Malware

The increasing threat of malware is also a concerning phenomenon in Australia. At the end of 2014, Trend Micro (an IT security provider) found that Australians clicked on more than 45.5 million malicious links during the third quarter, ranking Australia as the world’s fifth-most prolific ‘clicker’ of malicious links.

In addition, Trend Micro reported 14.4 million malware infections detected in Australia in the third quarter, an increase from 11.2 million infections in the first quarter.8

Victims are tricked into clicking on malicious links in a number of ways. One trend involves offenders sending malicious links contained in emails purporting to be from a legitimate source. In July 2015, the Australian Cyber Security Centre issued a warning to web users to be wary of malicious links contained in emails that appeared to be from Australia Post or the Australian Federal Police. The emails prompt users to download an archive file (.zip, .rar or .7z) that would encrypt information on the user’s computer, rendering it inaccessible unless a ransom was paid.9

In 2014, malware—including ransomware—was the predominant cybercrime threat in Australia. It has been identified as a persistent threat, because new malware types are developed and released regularly, and antivirus software cannot detect all new variants.10 The Australian Internet Security Initiative, facilitated by the Australian Communications and Media Authority, identified the three most problematic and widespread malware variants between April and December 2014 as Zeus, ZeroAccess and Conficker.11

Zeus12

Zeus has been identified as a Trojan virus that steals banking details through key-logging and form-grabbing. In June 2014, approximately 1 million computers worldwide were thought to be infected with Zeus with an estimated loss of USD $100 million. This ultimately led to a joint operation between the US Federal Bureau of Investigation (FBI) and the Australian Federal Police to take down the Zeus virus. Civil and criminal orders obtained by the United States allowed authorities to sever communications between Zeus and its command and control servers. This initiative ultimately led to the identification of the leader of a cyber-crime group based in Russia and the Ukraine responsible for the Zeus virus who is currently wanted by the FBI for a reward up to $3 million US.13

ZeroAccess14

ZeroAccess is a common type of malware in Australia that causes infected computers to commit ‘click-fraud’—that is, generating clicks on advertisements to receive commission from the company that owns the advertisement. The amount paid is dependent on the country in which the installation occurs, with
installations on Australian computers earning $75 USD. Australian Internet Security Initiative data suggests that ZeroAccess infected approximately 4,000 computers per day between October and December 2014. While ZeroAccess is primarily used for click-fraud and Bitcoin mining, the real concern is its ability to undertake any activity desired by whomever is controlling it. For example, in 2014, ZeroAccess affected Point of Sale systems in 60 Australian Pizza Hut stores, resulting in customers being unable to be served for a period of up to two hours, with some stores even closing for an entire day. Moreover, arguably even more problematic is the fact that ZeroAccess employs its own self-protection methods, disabling any security tool that attempts to identify or disable it.

Conficker\(^5\)

Conficker is a worm that exploits vulnerabilities in the Microsoft Windows operating system. It has been identified as a virus that is unusually difficult to counter, due to its use of multiple advanced malware techniques.\(^6\) Users are initially targeted on social networking websites such as Facebook and Twitter, and once a computer becomes infected, Conficker allows its controller to access personal information such as credit card numbers, passwords and other banking information.\(^7\) Although Microsoft and antivirus providers have released patches to remove the virus, the Australian Cyber Security Centre has identified that many computers still remain vulnerable and infected.

5.7.4 Ransomware

Ransomware refers to malicious software that attempts to extort its victim by locking or stealing a computer’s content and requiring a fee to be paid as a prerequisite for its return. The Australian Cyber Security Centre has identified cases where an infected computer has had its webcam activated, accompanied by a message from a law enforcement agency indicating that the victim’s computer has been used for illegal purposes and will result in an arrest unless a fine is paid.\(^8\)

This type of conduct was also seen in a UK study, where one participant who used the Internet frequently for business and leisure reported switching on his laptop one day and finding a message reading ‘[name of local police], you are in violation of a Great Britain law for looking at child abuse images (‘child porn’).’ The message was accompanied by a segment explaining that if a £100 fine was paid, no further action would be taken. In fact, the participant had not been accessing illegal pornography, and the message was the result of a virus. The user did, however, intend to pay the fine due to the potential damage to his reputation arising out of the false accusation made against him.\(^9\)

In these particularly vicious scams, payment is usually required by means of untraceable virtual currencies, such as Bitcoin.

Like malware, ransomware usually infects victims through emails purported to be from a legitimate source. However, the Australian Cyber Security Centre identified a case in 2014 when ransomware was infecting computers through compromised advertisements on websites that were frequently visited by Australians.

Ransomware was covertly installed on the victim’s computer by exploiting security vulnerabilities in Adobe Flash. The ransomware disabled the hard drive, which could only be re-enabled by the purchase of a decryption key. While the websites (hosting the advertisements) were not compromised, the advertising network connecting to the websites were found to have insufficient screening to detect advertisements originating from a malicious source.\(^10\)
5.7.5 Distributed Denial of Service

Distributed Denial of Service (DDoS) refers to the process of deliberately ‘flooding’ a network with more traffic than it can handle, thus disabling it. The effect is analogous to the difficulties encountered when using a mobile phone after a major sporting event or concert, when local cell phone towers are unable to handle the increased volume of traffic.

The Australian Cyber Security Centre has identified DDoS attacks as operating in a similar way to ransomware. That is to say, a high-profile web server (such as one belonging to a bank) might be threatened with a DDoS attack unless a fee is paid. The Australian Cyber Security Centre has identified DDoS attacks to extort funds as a current trend. It is a concerning move beyond traditional DDoS attacks that are usually designed by deviant individuals for no more than their nuisance value.21

5.7.6 Virtual currencies

The ACC notes that virtual currencies are increasingly used by ‘everyday’ Australians for legitimate purposes, such as currency speculation, purchasing goods and paying for services.22

However, alongside the growing acceptance of virtual currencies in the mainstream, their use is recognised as an emerging threat in the Australian criminal environment—for online purchases of illicit goods (for example: drugs, child exploitation material and identity/financial data), money transfers between criminals, and cybercrime. The Crime and Corruption Commission (CCC) noted in its submission that:

While there are legitimate uses for virtual currencies (e.g. Bitcoin), there is a significant amount of suspected illicit activity associated with the currency. Technology-based money laundering involving the exploitation of virtual currencies by organised crime groups has been identified overseas and has the potential to develop into a more significant issue in Queensland.23

David Lacey, Managing Director of iDcare, identified an increase in products available for purchase through Darknet marketplaces. In addition to the sale of illicit credit cards, Mr Lacey identified that PayPal, eBay and even iTunes accounts were available for sale.24 Mr Lacey, however, noted that the primary concern for his business was the sale of personal credentials, such as driver’s licenses, passports and Medicare cards.25 The ACC also sees forged documents, secret foreign bank accounts, money-laundering services, hacking techniques and phishing and spam tools as commodities available for payment using virtual currency.26

Detective Superintendent Brian Hay identified an increased use of virtual currencies, such as Bitcoin, as a means, for example, of extorting money from wealthy businesses through the use of ransomware. Detective Superintendent Hay alerted the Commission to an example of a business that had its data stolen by cybercriminals who subsequently demanded payment of a sum of money in Bitcoin to ensure its return.27 Upon payment, the offenders attempted to extort more money from the business and, when that was refused, threats against the children and families of executives of the company were made, using identifiable information stolen through the original data breach.28 Detective Superintendent Hay underscored the need for law enforcement to understand the future environment relating to the use of crypto-currencies by organised crime.

Virtual currencies are beginning to be regulated; however, these regulations vary significantly from country to country. In Australia, a recent report of the Economics References Committee supported a ‘wait-and-see’ approach to government regulation, while recommending close monitoring by government agencies and the establishment of a Digital Economy Taskforce to gather further information on the uses, opportunities and risks associated with virtual, or digital, currencies.

Further, the ACC is currently collecting intelligence on the threat posed by the criminal exploitation of virtual currencies as part of Making Australia Hostile to Serious and Organised Crime: Project Longstrike.29
notes the use of virtual currencies to facilitate illicit trade on the Darknet which, by its very nature, is a black market, and has stated that:

(It is very difficult to precisely determine the extent of its use but intelligence suggests that there continues to be significant use of the darknets by serious and organised criminal entities and those seeking to access illicit commodities.30

(Endnotes)

1 Transcript of hearing, Brian Hay, 21 July 2015, line 37, p. 146.
2 Transcript of hearing, Brian Hay, 21 July 2015, line 8, p. 147.
24 Transcript of interview, David Lacey, 2 July 2015, line 25, p. 10.
25 Transcript of interview, David Lacey, 2 July 2015, line 26, p. 10.


27 Transcript of interview, Brian Hay, 18 June 2015, p. 33.

28 Transcript of interview, Brian Hay, 18 June 2015, p. 33.


6.1 Introduction

The Commission’s Terms of Reference required the Commission to inquire into the extent that money laundering facilitates or enables organised crime.1

Money laundering can be described as the process that criminals use to conceal their illicit profits, and to avoid prosecution, conviction, and confiscation of the proceeds of crime by authorities.7

The Australian Crime Commission (ACC) states that:

Money laundering is an intrinsic enabler of serious and organised crime. Organised crime groups rely on it as a way of legitimising or hiding the proceeds of their criminal activities. Money laundering is carried out at all levels of sophistication by most, if not all, organised crime groups.3

Money laundering has been repeatedly identified as a key enabler for organised crime entities throughout Australia. It is considered to be a critical risk to Australia for a number of reasons, including its ability to undermine the financial system in Australia and to corrupt individuals and businesses.4

Given the prevalence of money laundering and organised crime throughout the world, it is increasingly the case that money laundering is becoming a transnational enterprise, with profits from crime generated in Australia often being laundered throughout a number of countries.5

The United Nations Office on Drugs and Crime (UNODC) produced a research report in 2011, attempting to shed light on the total amounts of illicit funds generated by drug trafficking and organised crime that were likely to be laundered across the globe.6

UNODC noted the International Monetary Fund’s widely quoted 1998 consensus range that two to five per cent of global gross domestic product (GDP) is laundered money. UNODC’s meta-analysis of the results from various studies suggested that, for 2009, all criminal proceeds are likely to have amounted to 3.6 per cent of GDP, and that 2.7 per cent of GDP was available for money laundering through the financial system.7

The Commission notes that the global GDP for 2014 was USD$77,868.8 billion,6 and, therefore, based on UNODC’s conclusions in its 2011 report, USD$2,102.5 billion would represent the amount of criminal proceeds available for money laundering.

It has been noted that Australia is one of the largest financial markets in the Asia-Pacific region, which makes it very susceptible to money laundering.9
The ACC conservatively estimates that serious and organised crime costs Australia $15 billion every year. This cost comprises loss of business and taxation revenues, expenditure on law enforcement and regulatory efforts, and social and community impacts of crime.10

6.2 Legislation

6.2.1 Offences

Queensland

In Queensland, the offence of money laundering is found in section 250 of the Criminal Proceeds Confiscation Act 2002 (Qld). This section provides two offences: knowingly engaging in money laundering (which carries a maximum penalty of 20 years imprisonment or 3000 penalty units11) and recklessly engaging in money laundering (which carries a maximum penalty of 10 years imprisonment or 1500 penalty units12). Section 250 is reproduced below:

(1) A person who engages in money laundering commits a crime. Maximum penalty—
(a) for knowingly engaging in money laundering—3000 penalty units or 20 years imprisonment; or
(b) for recklessly engaging in money laundering—1500 penalty units or 10 years imprisonment.

(2) A person engages in money laundering if the person knowingly or recklessly—
(a) engages, directly or indirectly, in a transaction involving money or other property that is tainted property; or
(b) receives, possesses, disposes of or brings into Queensland money or other property that is tainted property; or
(c) conceals or disguises the source, existence, nature, location, ownership or control of tainted property.

(2A) For subsection (2), a person knowingly does an act mentioned in subsection (2)(a), (b) or (c) in relation to property (knowingly engaging in money laundering) if the person knows, or ought reasonably to know, that the property is tainted property or is derived from some form of unlawful activity.

(2B) For subsection (2), a person recklessly does an act mentioned in subsection (2)(a), (b) or (c) in relation to property (recklessly engaging in money laundering) if—
(a) the person is aware there is a substantial risk the property is tainted property or derived from some form of criminal activity; and
(b) having regard to the circumstances known to the person, it is unjustifiable for the person to take the risk.

(2C) The question whether taking a risk is unjustifiable is one of fact.

(3) In applying this section to a financial institution, the fact that the financial institution is, or has been, subject to a monitoring order or a suspension order must be disregarded.

(4) In this section—

- **tainted property** includes property that is tainted property because of an interstate confiscation offence.

Section 251(2) of the Criminal Proceeds Confiscation Act requires the Attorney-General’s written consent before a proceeding can be commenced (or heard and determined).13 This requirement will be addressed further below.
Money laundering

Division 400 of the Commonwealth Criminal Code establishes a number of money-laundering offences with differing maximum penalties, depending upon the amount of money or property involved and the relevant state of mind of the offender (referred to as *mens rea* at common law or the ‘fault element’ within the Commonwealth Criminal Code). A person can be guilty of money laundering if they are either intentionally committing the offence, or where they are reckless or negligent to the fact that the money or property is proceeds of crime or may become an instrument of crime.

The offences are outlined in the table below:

<table>
<thead>
<tr>
<th>Section 400.3</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>25 years imprisonment or 1,500 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>12 years imprisonment or 720 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>5 years imprisonment or 300 penalty units, or both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 400.4</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>20 years imprisonment or 1,200 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>10 years imprisonment or 600 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>4 years imprisonment or 240 penalty units, or both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 400.5</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>15 years imprisonment or 900 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>7 years imprisonment or 420 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>3 years imprisonment or 180 penalty units, or both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 400.6</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>10 years imprisonment or 600 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>5 years imprisonment or 300 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>2 years imprisonment or 120 penalty units, or both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 400.7</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>5 years imprisonment or 300 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>2 years imprisonment or 120 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>12 months imprisonment or 60 penalty units, or both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 400.8</th>
<th>Maximum penalty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believes the money or property to be proceeds of crime or intends that the money or property will become an instrument of crime</td>
<td>12 months imprisonment or 60 penalty units, or both</td>
</tr>
<tr>
<td>Reckless as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>6 months imprisonment or 30 penalty units, or both</td>
</tr>
<tr>
<td>Negligent as to fact that the money or property is proceeds of crime or the fact that there is a risk that it will become an instrument of crime</td>
<td>10 penalty units</td>
</tr>
</tbody>
</table>
Additionally, section 400.9 of the Commonwealth Criminal Code provides that a person commits an offence if:

(a) the person deals with money or other property; and
(b) it is reasonable to suspect that the money or property is proceeds of crime; and
(c) at the time of the dealing, the value of the money and other property is $100,000 or more.

The maximum penalty for that offence is three years imprisonment or 180 penalty units, or both.

6.2.2 Reporting regime

In addition to money-laundering offences, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act) and the Financial Transactions Reports Act 1988 (Cth) provide reporting obligations for specified entities or persons who deal with money.

The Financial Transactions Reports Act requires entities that satisfy the definition of a ‘cash dealer’ to report to the Australian Transaction Reports and Analysis Centre (AUSTRAC) any suspicious cash transactions,14 cash transactions of $10,000 or more,15 and international funds transfer instructions.16 In addition to cash dealers, there is also an obligation upon solicitors to report transactions involving $10,000 cash or more to AUSTRAC.17 The obligations in the Financial Transactions Reports Act do not apply to a transaction to which the AML/CTF Act applies.

The AML/CTF Act ‘forms part of a legislative package which implemented reforms to strengthen Australia’s AML/CTF regulatory regime and bring it into line with international standards set by the Financial Action Task Force (FATF).’18 Formed in 1989, the FATF is an independent, inter-governmental body, comprising 34 member nations. It develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction.

In October 2003, the FATF published 40 recommendations for combatting money laundering. Member nations participate in peer reviews to assess levels of implementation of the FATF recommendations. The enactment of the AML/CTF Act was a consequence of the FATF’s 2005 Mutual Evaluation Report on Australia.

The AML/CTF Act broadened the net in terms of entities required to report to AUSTRAC. It has also imposed additional obligations upon those entities. The Act sets out the primary obligations of ‘reporting entities’20 who provide ‘designated services’20 in the financial services sector, gambling sector and bullion dealer sector. The reporting entities include banks and credit unions, stockbrokers, financial planners, casinos, betting agencies, money remitters and bullion dealers. They must fulfil certain obligations when they provide designated services. Those obligations include:

- customer identification and verification of identity
- record-keeping obligations
- establishment of an anti-money laundering and counter-terrorism financing program to minimise the risk of money-laundering or terrorism-financing activities being conducted within their organisation
- ongoing customer due diligence and reporting of suspicious matters, threshold transactions and international funds transfers.

In July 2007, the Commonwealth Attorney-General’s department announced that the second tranche of the legislation would impose similar obligations on lawyers, notaries, other independent legal professionals, accountants, real estate agents, dealers in precious metals and stones, and trust and company service providers who are collectively referred to as ‘designated non-financial businesses and professions’.21 However, the second tranche of the legislation is yet to be implemented. Amendments were deferred to 2011 due to the impact of the global financial crisis on business and the expected cost of compliance. To date, no amendments have been made.
Australia was the subject of a further FATF mutual evaluation in 2014, and in April 2015, the Anti-money laundering and counter terrorism financing measures Australia: Mutual Evaluation Report was published. One of the key findings of that review was:

Most designated non-financial business and profession sectors are not subject to AML/CTF requirements, and did not demonstrate an adequate understanding of their [money laundering and terrorist financing] risks or have measures to mitigate them effectively. This includes real estate agents and lawyers, both of which have been identified to be of high ML [money-laundering] risk in Australia’s National Threat Assessment.22

Throughout the report, criticisms were made of the failure to enact the second tranche of the AML/CTF Act. The assessment team found that there were limited measures in place to mitigate the high risks associated with the abuse of legal entities and corporate structures. It is believed that obligations imposed on professional facilitators to record details about the beneficial ownership of companies and trusts and to report suspicious transactions would not only enhance detection of money-laundering or terrorism-financing activity, but would also facilitate the timely tracing of criminal assets.23 The failure to enact the second tranche of legislation will be addressed in further detail in this chapter, when referring to professional facilitators.

A further key finding of the mutual evaluation was that, despite the good-quality financial intelligence held by AUSTRAC and disseminated to law enforcement agencies, there is a ‘somewhat limited use of AUSTRAC information by law enforcement as a trigger to commence [money laundering and terrorist financing] investigations.’ This was thought to present a weakness in the Australia’s AML/CTF regime.24

Obligations under the Anti-Money Laundering and Counter Terrorism Financing Act

Customer identification and verification of identity

Customer due diligence requirements are contained in both the AML/CTF Act and the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). New customer due diligence requirements were enacted through amendments to seven chapters of the AML/CTF Rules, with an implementation period to run from 1 June 2014 to 31 December 2015.

Before providing a designated service, reporting entities must verify a customer’s identity under section 32 of the AML/CTF Act. Under section 33 of the Act, certain ‘special circumstances’ can be prescribed in which a designated service may be provided to a customer before the verification of their identity. Unless an exception applies, a failure to verify a customer’s identity prior to providing a designated service could result in a pecuniary penalty of up to and including 100,000 penalty units for a body corporate, or not more than 20,000 penalty units for a person that is not a body corporate under section 175(4) and (5) of the AML/CTF Act. Where a designated service has commenced without verifying the customer’s identity due to ‘special circumstances’, section 34 provides a timeframe in which the customer’s identity must be ascertained by the reporting entity. Continuing to provide a designated service to the customer, without verification of their identity within the relevant timeframes, also attracts a pecuniary penalty.

Under section 30 of the AML/CTF Act, a reporting entity that is taken to be a ‘low-risk designated service’ under the AML/CTF Rules is not required to carry out the applicable customer identification procedures, unless, under section 31(2) of the Act, a suspicious matter reporting obligation arises in regard to a customer, in which instance the reporting entity must carry out identification and verification procedures in accordance with Part 6.4 of the Rules.

Chapter 4 of the AML/CTF Rules prescribes the procedures to be included in a reporting entity’s money-laundering and counter-terrorism program (AML/CTF program) for verifying the identity of different types of customers—including individuals, companies, trustees, partners, associations, registered co-operatives, government bodies, beneficial owners and politically exposed persons. These procedures generally require reporting entities to have risk-based systems and controls in place to reasonably satisfy themselves that the customer is who they say they are, or, in the circumstances of a body corporate, that the entity exists and that
the reporting entity has sufficient information regarding the body corporate. The AML/CTF Rules also outline
different pieces of information that must, as a minimum, be collected from different types of customers, and
require reporting entities to have a methodology for verifying the identity of different types of customers,
based on information and documents relevant to the type of customer.

The reporting entity’s AML/CTF program (required under section 81 of the AML/CTF Act) must also have a
procedure to verify the customer’s name and either their date of birth or residential address. This verification
must be based on reliable and independent documentation, or reliable and independent electronic data, or
a combination of the two. The AML/CTF program should also have systems and controls to determine when
additional information collected from a customer should be verified.

In the event that a discrepancy arises during the course of the verification process, the AML/CTF program
must include risk-based systems and controls for the reporting entity to determine whether it is reasonably
satisfied that the customer is the person that they claim to be.

In circumstances where a customer is considered to be a medium or lower money-laundering or terror-
financing risk, a reporting entity can apply a more simplified procedure to verifying their identity. This
includes, under part 4.2 of the AML/CTF Rules, verifying the customer’s residential address, date of birth,
or both, from an original or certified copy of a primary photographic identification document, or from
an original or certified copy of a primary non-photographic identification document plus an original or
certified copy of a secondary identification document. The documentation must not be expired. A simplified
procedure for electronic verification can also be used for medium-to-lower-risk customers.

Record-keeping obligations

There are a number of record-keeping obligations under the AML/CTF Act. Under section 106, the AML/
CTF Rules may provide that certain records must be made and kept by a reporting entity about the provision
of designated services to a customer. Under section 107 of the Act, where a reporting entity makes a record
regarding the provision of designated service to a customer, and the Rules do not declare that record to
be exempt from section 107, then the reporting entity must retain the record or a copy of the record, or an
extract of the record that contains prescribed information, for a period of seven years after the making of the
record. A reporting entity that fails to comply with section 107 could be subject to a pecuniary penalty.

Other requirements to retain information apply to:

- documents provided by a customer relating to the provision or prospective provision of a service
  (section 108)
- documents relating to certain authorised deposit-taking institution accounts (sections 109 and 110)
- records regarding customer identification procedures (sections 111 to 114)
- information about electronic funds transfers (section 115)
- records regarding the adoption of AML/CTF programs (section 116)
- records about due diligence of correspondent relationships (section 117).

Establishment of an AML/CTF program

Under section 81 of the AML/CTF Act, a reporting entity must adopt and maintain an AML/CTF program
before it provides a designated service to a customer. A failure to adopt and maintain such a program prior
to providing a service may incur a pecuniary penalty of not more than 100,000 penalty units for a body
corporate, or not more than 20,000 penalty units for a person that is not a body corporate under sections
175(4) and (5) of the Act. There are three different types of programs that can be adopted by a reporting entity
under sections 84, 85 and 86 of the Act. An entity can adopt a standard program under section 84, a ‘joint’
program under section 85, or a ‘special’ program under section 86.

A ‘standard’ program consists of two parts under section 84 of the AML/CTF Act: Part A and Part B. Part A
of a standard program has the purpose of identifying, mitigating and managing the risks the reporting entity
may face that the provision of the designated services could facilitate money laundering or the financing
Money laundering

Queensland Organised Crime Commission of Inquiry

of terrorism. Part B of the standard program has the purpose of setting out the customer identification procedures for the reporting entity in compliance with any customer identification requirements in the AML/CTF Rules. A ‘joint’ program can be adopted by a reporting entity where that entity belongs to a ‘designated business group’. Under section 85, a ‘joint’ program applies to all reporting entities that belong to the designated business group. The requirements, for the most part, mirror those of a standard program, except that the joint program may make different provisions with respect to different reporting entities.

Ongoing customer due diligence

Section 36 of the AML/CTF Act requires a reporting entity to monitor its customers on an ongoing basis to identify, mitigate and manage the risk that the designated service may involve or facilitate money laundering or the financing of terrorism. The reporting entity must do this in compliance with any relevant provisions contained in the AML/CTF Rules. A failure to perform ongoing customer due diligence under section 36 of the Act could result in a pecuniary penalty.

Chapter 15 of the Rules requires a reporting entity’s program to have appropriate risk-based systems and controls to allow the entity to determine when further information or beneficial owner information should be collected or verified in respect of customers or beneficial owners to enable the review and update of information for ongoing customer due diligence purposes. Under Part 15.3 of the Rules, a reporting entity must take reasonable measures to keep, update and review documents, data or information collected under the customer identification procedures particularly in relation to high-risk customers.

Reporting of suspicious matters

Under section 41 of the AML/CTF Act, a reporting entity must provide a report to AUSTRAC when a suspicious matter reporting obligation arises. A suspicious matter reporting obligation arises when a reporting entity either provides or proposes to provide a designated service to a person or is requested to provide the service to a person and the service is the kind of service the entity usually provides and a number of different scenarios arise. The scenarios that give rise to a suspicious matter reporting obligation in these circumstances include:

- the reporting entity suspects, on reasonable grounds, that the person or agent of a person is not who they say they are
- the reporting entity suspects, on reasonable grounds, that information regarding the provision of the service or prospective provision of the service would be relevant to the investigation or prosecution of a person for an offence against a law of the Commonwealth or of a state or territory, including an investigation or prosecution for tax evasion or attempted tax evasion
- the reporting entity suspects, on reasonable grounds, that the information regarding the provision of the service or prospective provision of the service would be of assistance in the enforcement of the Proceeds of Crime Act 2002 (Cth) and its regulations or a corresponding state or territory act
- the reporting entity suspects, on reasonable grounds, that the provision or prospective provision of the services is preparatory to the commission of an offence under certain parts of the definitions of financing of terrorism or money laundering in section 5
- the reporting entity suspects, on reasonable grounds, that information that the reporting entity has concerning the provisions or prospective provision of the services may be relevant to a prosecution of a person for an offence covered by certain parts of the definition of financing of terrorism or money laundering in section 5 of the AML/CTF Act.

Under section 41(2) of the AML/CTF Act, when a suspicious matter reporting obligation arises, the reporting entity has three business days after the entity forms the relevant suspicion to inform AUSTRAC about the matter. However, if the matter relates to a suspicion that the act is preparatory to the financing of terrorism, or that information held by the entity may assist in an investigation into or a prosecution of a person for financing of terrorism, the entity must report it within 24 hours of forming the relevant suspicion. A failure to report a suspicious matter within the relevant timeframes attracts a pecuniary penalty.
Reporting threshold transactions

Under section 43 of the AML/CTF Act, a reporting entity must report to AUSTRAC a ‘threshold transaction’ within 10 business days after the transaction takes place. A ‘threshold transaction’ for the purposes of section 43 means a transaction involving the transfer of physical currency or e-currency of $10,000 or more, or if the regulations provide that a type of transaction is a ‘threshold transaction’.

Reporting international funds transfers

Pursuant to section 45 of the AML/CTF Act, a person (which includes a body corporate or other entity) who is the sender of an international funds transfer instruction transmitted out of Australia or the recipient of an international funds transfer instruction transmitted into Australia must report information about that instruction to AUSTRAC within 10 business days of receiving that instruction.

Under Chapter 16 of the AML/CTF Rules, a report to AUSTRAC about the international funds transfer instruction must include, where there is an electronic funds transfer instruction received by an Australian institution to transfer money to be made available to a recipient from an institution in a foreign country, information such as:

- the name of the ordering institution
- the name of the institution transmitting the instruction to a beneficiary, or ‘receiving’ institution
- if applicable, the sender’s branch or department that received the instruction
- the date the sender transmits the instruction to the beneficiary institution
- the name of the beneficiary institution and the name of the branch or department of the beneficiary institution at which the funds will be made available to the payee
- the name of the payee and other relevant information about them, including the number of their bank account, their address, and other identification information as applicable
- directions provided by the payer to the payee
- the name or identity of any interposed institution in the funds transfer chain
- the name or identity and account number of any institution through which the beneficiary institution will be reimbursed,
- any other details regarding the instruction
- the amount referred to in the instruction
- the currency of the amount referred to
- the date on which the money becomes available to the payee.

Information of a similar nature is required where an electronic funds transfer instruction is accepted in a foreign country for transferred money to be made available to a payee through an Australian institution.

In 2013, AUSTRAC and the Attorney-General’s Department reported a growth in offshore service providers, who are not regulated under the AML/CTF Act because they do not satisfy the ‘geographical link’ requirement under the Act. Offshore-based online remitters and virtual currency exchanges are examples of entities falling outside the reporting regime. The Queensland Police Service (QPS) had raised this as a specific issue in relation to lost intelligence on Western Union transfers, when Western Union moved their servers offshore (see discussion in the section titled Financial data theft). Given the current review of the AML/CTF Act, an amendment to the legislation seems likely to ensure that those transactions with an Australian connection are captured. The Commission supports any recommendation for such change.
6.2.3 The requirement to obtain the consent of the Attorney-General to charge the Queensland offence of money laundering under the State legislation

Section 250 of the Criminal Proceeds Confiscation Act requires the consent of the Attorney-General for a prosecution under that section to proceed. That requirement is not peculiar to the offence of money laundering. In fact, prosecutions for the following offences under Queensland’s Criminal Code also require the Attorney-General’s consent in order to commence:

- Section 54A: Demands with menaces upon the agencies of government
- Section 131: Conspiracy to bring false accusation
- Section 132: Conspiracy to defeat justice
- Section 415: Extortion with a circumstance of aggravation
- Section 541: Conspiracy to commit a crime
- Section 542: Conspiracy to commit other offences
- Section 543: Other conspiracies.

QPS Deputy Commissioner Ross Barnett advised the Commission that the QPS generally relied on the money-laundering provisions contained in the Commonwealth Criminal Code instead of the Queensland offences, because the federal provisions did not require ministerial consent for the proceedings. He said that the federal regime was a ‘more efficient process for investigators’.26

The Queensland Acting Director of Public Prosecutions, Mr Michael Byrne QC, provided some thoughts on this issue in a submission to the Commission:

The process for obtaining consent requires the preparation of an application, and often a brief of evidence. That application and brief is usually submitted to the ODPP for the provision of advice to the Attorney-General. That process contributes to delay in the prosecution, and sometimes charging, of suspected offenders. There have been a total of 47 applications received by ODPP in the period 1 January 2010 to 31 March 2015.27

The Acting Director of Public Prosecutions submitted that the legislation should be amended to remove the requirement for the consent of the Attorney-General in these prosecutions.

The Crime and Corruption Commission (CCC) advised this Commission that the need to obtain ministerial consent to lay a money-laundering charge was unique to this state. The CCC noted that the consent requirement necessitated the preparation of a full brief of evidence for submission to the Minister, with no guarantee that consent would be given. The CCC is of the view that the requirement to obtain consent from the Attorney-General should be removed.

Notices were issued to the Queensland Office of the Director of Public Prosecutions (ODPP) and the Commonwealth Office of the Director of Public Prosecutions (CDPP) to determine the number of money-laundering offences charged under the respective legislation within Queensland in the period 1 January 2012 to 31 August 2015.

The Queensland Acting Director of Public Prosecutions advised the Commission that, during this period, it had presented five indictments, charging a total of ten persons with offences of money laundering pursuant to section 250 of the Criminal Proceeds Confiscations Act. Of those matters, the prosecution of four persons had been finalised (all in the one indictment) with two proceeding by way of a plea of guilty, and two being discontinued, having pleaded guilty to other offences.28

Mr David Adsett, Commonwealth Deputy Director of Public Prosecutions, advised the Commission that during this period, the CDPP had presented:

- one indictment charging a person with an offence against section 400.3 of the Commonwealth Criminal Code—although that particular count on the indictment was subsequently discontinued.
• five indictments charging persons with an offence against section 400.4 of the Commonwealth Criminal Code—of those indictments, four have been finalised by pleas of guilty and one remains outstanding
• three indictments charging persons with an offence against section 400.5 of the Commonwealth Criminal Code—those indictments have all been finalised by way of pleas of guilty
• two indictments charging two people with an offences against section 400.6 of the Commonwealth Criminal Code—both indictments were finalised by way of pleas of guilty
• no indictments in the relevant period charging persons with offences against sections 400.7 or 400.8
• two indictments charging persons with offences against section 400.9 of the Commonwealth Criminal Code—of those indictments, one was finalised by way of a plea of guilty and the other was acquitted after a trial.  

In total, therefore, 13 indictments have been presented under the Commonwealth legislation in this period.

The Commission is also aware that a number of Commonwealth money-laundering charges were finalised in the Magistrates Court, arising out of QPS’ Operation Kilo Dictate. The schedule provided to the Commission by the CDPP contained a list of 19 matters finalised in that Court, with charges under section 400.6(2) of the Commonwealth Criminal Code. See the case study of *R v Stroia* and associated offenders in the section on financial data theft, above.

Historically, ministerial consent to a prosecution would be required to deter private prosecutions brought in inappropriate circumstances, and to provide an additional safeguard for those offences that covered sensitive or controversial areas, or where the offence was broadly drafted, potentially applying beyond the mischief aimed at.  

The Commission has considered the money-laundering offences contained in section 250 of the Criminal Proceeds Confiscation Act (Qld) and is satisfied that such reasons for requiring ministerial consent are not present with regards the Queensland money-laundering offences. The Commission agrees with the Acting Director of Public Prosecutions, the CCC and the QPS that the consent requirement should be removed.

**Recommendation**

6.1 The Commission recommends that the Queensland Government amend section 251 (Charging of money laundering) of the *Criminal Proceeds Confiscation Act 2002*, to remove the requirement for Attorney-General consent.

**(Endnotes)**

1 Commissions of Inquiry Order (No. 1) 2015, paragraph 3(d).


Money laundering

Queensland Organised Crime Commission of Inquiry


Section 250(1)(a) *Criminal Proceeds Confiscation Act 2002* (Qld).

Section 250(1)(b) *Criminal Proceeds Confiscation Act 2002* (Qld).

Section 251(2), (3) *Criminal Proceeds Confiscation Act 2002* (Qld).

Section 16 *Financial Transaction Reports Act 1988* (Cth).

Section 7 *Financial Transaction Reports Act 1988* (Cth).

Section 15 *Financial Transaction Reports Act 1988* (Cth).


Section 5 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

Section 6 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).


Statutory declaration of Ross Barnett, 1 June 2015.

Submission of Office of Director of Public Prosecutions, 29 May 2015, pp. 11–12.

Statutory declaration of Michael Byrne, 10 September 2015.

Affidavit of David Adsett, 10 September 2015.

6.3 How is money laundered?

There are a number of different strategies that organised crime groups can use to make their proceeds of crime appear legitimate. Typically, money goes through a three-stage process in order to hide the source of the illicit funds. These cycles are:

1. ‘Placement’ – the first phase of the cycle in which money is placed into a formal financial system such as a bank account
2. ‘Layering’ – the part of the process in which a number of different financial transactions are made, such as moving or transferring the funds around different banks, accounts, trusts and corporations, to conceal their original source
3. ‘Integration’ – the final stage in which the funds appear to have been acquired through a legitimate source. At this stage, funds can be invested into legitimate business, used to buy real estate or other assets and goods, or put back into funding criminal activities.

To achieve ‘integration’, organised crime groups can use a number of different methods, or ‘channels’. In many instances, more than one channel is used in the money laundering cycle.

There are a number of channels used by those laundering money to achieve their desired effect. The money laundering channels that the Commission focused on are:

- the banking sector
- alternative remittance systems
- the casino and gaming industry
- debit cards
- the precious stone, jewellery and bullion trade
- the purchase of real estate
- the establishment of corporate structures and trusts
- professional facilitators—including lawyers and accountants who may establish corporate structures and trusts that are used to launder money through Australia and overseas.

Another common method of money laundering is through using businesses and corporations to both distance organised crime groups from the profits of crime, and as a way of legitimising the illicit funds. Businesses may be a simple ‘front’ for money laundering, or a legitimate business may be operated but used to launder the funds through inflation or other manipulation of the businesses revenue.

6.3.1 Banking

Most funds that go through the money-laundering cycle are, at some stage, placed within the banking system. As such, one way in which money can be laundered is through manipulating the banking sector. Organised crime groups can do this by:

- opening accounts under false names or through identity fraud
- using the bank accounts of third parties such as family or ‘money mules’ to distance themselves from money laundering transactions
- making multiple small deposits at different banks and branches to avoid bank reporting requirements and to minimise suspicion
- using ‘wire transfers’ to move the money quickly to accounts in other countries where anti-money laundering regimes are poor
- using complex corporate ownership structures and transferring funds between different entities and jurisdictions
• taking out loans that are repaid with proceeds of crime
• using bank drafts, promissory notes, traveller’s cheques and money orders (often referred to collectively as ‘bearer negotiable instruments’) to move money discreetly between countries
• using safe deposit boxes to store proceeds of crime.  

One way in which banks can be manipulated is through the use of ‘money mules’. These are people who may be recruited unwittingly to assist criminal organisations in moving funds between accounts. To obtain the cooperation of these third parties, money launderers pose as a company seeking a ‘financial agent’ or ‘fund manager’. They can do this via email offers or online recruitment websites. Once a person agrees to accept the position, they either open up a new bank account to receive the funds, or give the ‘employer’ their own bank account details to receive the funds. Once the funds are received, they send them on to a final destination, usually offshore.7

The following case study details an offender who actively sought work as a ‘money mule’:

---

### Case study

**R v Columbus**8

Columbus pleaded guilty to two counts under the Commonwealth Criminal Code: one count of dealing in proceeds of crime worth $10,000 or more under section 400.6, and one count of using a telecommunications network with intent to commit a serious offence under section 474.14(1).

Columbus and his partner contacted a company online. The company agreed to transfer unlawfully obtained money into accounts established by Columbus and his partner. A total of about $38,427.12 was paid into his accounts. Columbus withdrew cash and sent it to an address in Singapore, after retaining a commission of approximately 5 per cent. The banks recovered about $19,644.12. Emails located on Columbus’ laptop indicated that he had sent emails looking for further work as a ‘mule’, between January and March 2006.

Columbus had no record of previous criminal activity, and had a good educational and work history.9 He was sentenced to concurrent terms of 15 months imprisonment for each offence (not disturbed on appeal).

---

Another method of money laundering, discussed in the case study below, is the recruitment of people through online dating sites. This technique can be difficult for law enforcement agencies to detect, as people recruited through online dating sites are often honest people with no idea that they are involved in money laundering, who often have no criminal history and would not come under scrutiny from financial institutions.10
Case study

Money mule

An Australian man was recruited as a ‘money mule’ through an online dating website. It was his belief that he was talking to a person in Russia who would become his wife. In an email, he was told that the woman’s sister in Australia wished to transfer funds to his potential wife in Russia. He was asked by his potential bride to set up a bank account at the same institution as the woman’s sister. Proceeds of crime were then transferred into this account, with the ‘mule’ believing that the deposits were being made by the ‘sister’. The first deposit was withdrawn in cash and sent to Russia by remittance agency Western Union. The second deposit was seized by law enforcement officers.\(^{11}\)

6.3.2 Alternative remittance systems

Another method that organised criminal groups can use to make their funds legitimate is through services known as ‘alternative remittance systems’. These are services that exist outside of the formal banking system, and they are a way of moving funds around internationally without the need for organised crime groups to physically transfer the funds overseas. In addition to using their services in the traditional manner to send funds, they can also use the services of unregistered alternative remittance agents who conduct their business ‘on the side’, making payments more difficult to track. They can also be used by organised crime groups through a laundering technique known as ‘cuckoo smurfing’.\(^{12}\)

Alternative remittance services work by means of an agent in one location entering into agreements with agents in other locations.\(^{13}\) When a person wishes to send funds overseas using this system, they approach an alternative remittance system agent, who takes the funds they wish to transfer. The agent then calls one of their contacts in the overseas region and tells them to pay the required amount to the intended recipient.\(^{14}\) The agent then owes a debt to the other agent, which may be re-paid as agreed between the agents—in other words, they may pay their debts on a monthly basis, by invoice, and so on.\(^{15}\)

The remittance sector has obligations under the AML/CTF Act and the AML/CTF Rules. Under section 74 of the Act, remittance services cannot be provided unless they are registered. Section 75C provides the circumstances under which AUSTRAC must register a person as a remittance network provider, an independent remittance dealer, or a remittance affiliate of a registered remittance network provider. Section 74(2) provides that a person commits an offence where they provide a registrable designated remittance service and they are not registered, or where they provide the service in breach of a condition on their registration. A person may be liable for two years imprisonment, 500 penalty units, or both.

Under section 6, table 1 of the AML/CTF Act, those who give effect to remittance arrangements under a designated remittance arrangement, or who operate a remittance network service, are providing a designated service, and are reporting entities under the Act. This means that they are bound by reporting obligations such as reporting suspicious matters under section 41, reporting threshold transactions under section 43 and reporting international funds transfer instructions under section 45. They are also required to adopt an AML/CTF program. If they are a registered remittance network provider, then they must make their standard AML/CTF program available to their registered affiliates for the purpose of adoption and maintenance. A failure to provide their AML/CTF program to affiliates could result in a pecuniary penalty under sections 84(5A) and (5B) of the AML/CTF Act.

A recent issue has arisen with the ‘de-banking’ of independent remittance service providers. The Commonwealth Joint Committee on Law Enforcement concluded its Inquiry into financial related crime
Money laundering and published its report in September 2015. The Committee heard that major Australian banks were using changes to international AML/CTF arrangements to justify the closure of remitters’ Australian operating bank accounts, and were doing so while still offering their own remittance services.16 The Committee did not make any recommendations, given the complexity of the issue and the establishment of an Attorney-General’s Department working group to consider it. The Committee did suggest that a suitable balance needs to be struck ‘between the constraints of a robust AML/CTF regime and the ability for legitimate remittance service providers to access necessary financial products’.17

Although alternative remittance services are legal, there a number of people who may run such a business ‘on the side’ of a legitimate business.18 They may do this to avoid reporting requirements and scrutiny under the AML/CTF Act. These services may be particularly attractive for those wishing to engage in money laundering. For example, an alternative remittance agent may send $50,000 worth of goods to another alternative remittance agent. However, they may only invoice that agent for $30,000 worth of goods. They then provide an instruction to pay $20,000 on behalf of their client to a recipient in that jurisdiction. In this manner, $20,000 worth of value has been transferred out of the country to the second agent, without the agent in the original jurisdiction ever explicitly sending funds.19

Another way in which alternative remittance services can be used for money-laundering purposes is through a technique known as ‘cuckoo smurfing’. This method involves an alternative remittance agent taking on a legitimate request to transfer funds to an overseas source. The agent then provides the details of the transaction to an organised crime group, who use the cash they have received through criminal activities to pay the money into the account that was legitimately requested by an unknowing third party. The alternative remittance service dealer then provides the same amount of funds to the organised crime group. Detailed below are two examples of cuckoo smurfing operations that have been identified in Australia by law enforcement authorities.

Case study

Majeed v The Queen20

In this case, the appellant was charged under section 400.3(2) of the Commonwealth Criminal Code for dealing with money, of a value of $1,000,000 or more, being the proceeds of crime, and being reckless as to the fact that the money was the proceeds of crime.

The appellant had been sentenced in the County Court of Victoria to seven years imprisonment with a five year non-parole period for his role in a money-laundering scheme that involved twelve laundering transactions, totalling $5.2 million over a five-year period.

The prosecution alleged that the money dealt with by the appellant was the proceeds of ‘ecstasy’ trafficking, performed by a criminal syndicate. The syndicate received approximately 1,200,000 ‘ecstasy’ tablets in Melbourne in February, March and May of 2008, which were sold to wholesale customers across Australia. The proceeds of these sales were then required to be sent to the ‘ecstasy’ suppliers in Europe.

The appellant was a representative of an international money remitter. The appellant liaised with the criminal syndicate to provide them with details of bank accounts in which cash was to be deposited. Members of the syndicate would then make deposits into the bank accounts, and confirm with the appellant that those deposits had been made. Once confirmed, the appellant would arrange for an overseas remitter to release cash to the European suppliers, to whom the syndicate owed money for the drugs.

The appellant and other participants in the money-laundering scheme were paid a commission by the syndicate. The appellant, in this instance, received $28,000 for his part in the scheme.
Cuckoo smurfing

In 2013, AUSTRAC reported on an alleged cuckoo-smurfing operation. In the investigation, a money-laundering syndicate attempted to use the technique to launder $1.75 million dollars in illicit drug proceeds.

In this matter, a legitimate customer of an alternative remittance service attempted to transfer $1.75 million to his daughter, who was studying in Australia. The customer transferred the money to the alternative remittance service and provided them with the bank account details of his daughter.

The alternative remittance dealer contacted members of a criminal syndicate and gave them the details of the intended recipient’s bank account. The syndicate then proceeded to deposit their proceeds of crime into that bank account across a number of bank branches in New South Wales and Victoria, ultimately providing the required $1.75 million dollars over a six-week period.

The remittance dealer then transferred $1.75 million from the customer’s original deposit, which was ‘clean’ money, to another bank account associated with the syndicate.

Australian bank staff notified AUSTRAC of suspicious transactions because those depositing on the money were reluctant to provide their details when making the deposits, including by writing ineligibly and not providing full names.

6.3.3 Casinos

The casino and gaming industry is another sector that can be exploited for the purposes of money laundering. Money can be laundered through these organisations in a number of ways, including by people using proceeds of crime to ‘buy in’ and then cashing out their chips or ‘winnings’, through casino junkets where casinos have minimal interactions with the individual gamblers, and through conducting business with casino chips.

Casinos, as organisations that engage in gambling services, also have obligations as designated services under the AML/CTF Act.

AUSTRAC has noted that the gaming sector, in general, was particularly used in the ‘placement’ and ‘layering’ stages of the money-laundering cycle. One of the reasons given for the attractiveness of the gambling sector to money launderers is the high cash turnover and the sheer volume of transactions that occur within the Australian gambling industry.

One way in which casinos can be used to legitimise illicit funds is through exchanging cash for casino chips. The chips are then cashed as ‘winnings’, and the person has a receipt proving the legitimacy of the funds. In some instances, they are cashed out without the person playing. In other instances, funds may be placed through a slot machine, and then credits are claimed as a jackpot win. On some occasions, money launderers will use ‘mules’ or third parties to purchase and cash-in chips, to avoid raising suspicion and to distance themselves from transactions.

Casino junkets have also been noted by AUSTRAC as being another way that money launderers use casinos to legitimise their funds. Junkets are often tourism-based trips that are run by an operator. Gambling as part of these groups may make it difficult for casinos and law enforcement to determine the course of funds, as the operators usually facilitate the purchase and cashing-in of casino chips and manage other dealings with the casinos. This, therefore, minimises the face-to-face contact that individual players have with the venues, which limits the ability of the casino to adequately assess individual players.
Additionally, VIP and ‘high roller’ rooms can also be open to exploitation, due to the high value of the gambling that occurs in those environments.29

The Commission is aware that in New South Wales and Victoria, certain persons have been banned from entering casinos due to this behaviour.

NSW and Victorian police services seem to have been more active in banning known organised crime offenders, as a means of disrupting money laundering. In mid-2015, concerns were raised in the media that the absence of that regime in Queensland meant those persons banned in Victoria and New South Wales were being given ‘free rein at Queensland casinos’.30

Case study

Casinos

AUSTRAC reported that a person involved in importing heroin into Australia from Vietnam used casinos to launder the money. In some instances, he used third parties to purchase gaming chips on his behalf, and would cash out multiple times a day—usually in amounts that were below the $10,000 reporting threshold. The suspect also sent large cash payments to different entities in Vietnam, using a remittance dealer who had been non-compliant with their reporting obligations.31

Another example of casino money laundering is a case in which a suspect was arrested when collecting a package containing 3.4 kilograms of black opium resin. Further opium was found in connection with the suspect following the execution of search warrants. As part of the investigation, it became clear that the suspect was a regular casino patron. The person had chip cash-outs in the amount of $890,000, but there were few instances recorded of the individual playing.32

Case study

R v Yi-Hua Jiao33

In this case, a woman was charged under section 400.9(1) of the Criminal Code (Cth) for dealing with money, the value of which was more than $100,000, that it was reasonable to suspect was the proceeds of crime.

The facts of the matter are that the respondent flew from New Zealand to Sydney, where she was staying at The Star Casino. She met a man there with whom she exchanged a $5.00 note. It was alleged that this bank note had a known serial number, and this was a common method of identification for when cash was passed between members of criminal and money-laundering syndicates. After producing the $5.00 note, the respondent and the man went to the car park, where the man gave the respondent a sports bag. Evidence was given that they then attended a hotel room, where the bag was opened and it was found to contain Australian currency. The woman then went to the casino, where she deposited $624,340 into her ‘casino account’. A member of the casino staff gave evidence that the money was in poor condition, was soiled and gritty, and was not wrapped in a manner that was consistent with how a bank would wrap currency. The respondent then requested that the funds be transferred into a Brisbane Commonwealth Bank of Australia account held by a money remitter. The casino refused to make the transaction and contacted the police.
Lottery tickets

AUSTRAC has reported that a group of overseas nationals had been purchasing winning jackpot tickets from gamblers at clubs in Sydney. Over a one-year period, the group deposited $1.7 million of winning cheques, which they immediately withdrew in cash. It was believed that these tickets were purchased off the winners by using proceeds of crime.

6.3.4 Bullion and jewellery

Bullion is an attractive way to launder money as it has a high value and can be melted and turned into different forms. This makes bullion easy to conceal when it is being transported. In some instances overseas, bullion has been melted down and disguised as common items like nuts, bolts and wrenches.

Those who buy and sell bullion in the course of their business are bound by the provisions of the AML/CTF Act.

The purchase and sale of bullion is a ‘designated service’ under section 6 of the AML/CTF Act where it is bought or sold in the ‘course of carrying on a business’. Under section 5 of the Act, a reporting entity is a person who provides a designated service.

Under section 5 of the AML/CTF Act, bullion includes anything that, under the regulations, is taken to be bullion for the purposes of the Act. However, no regulations have been put in place to define bullion. AUSTRAC is of the view that bullion, for the purposes of the AML/CTF Act, could be considered to include gold, silver, platinum or palladium that has been authenticated to a specified fineness, evidenced by a commercially acceptable hallmark, stamping or other authenticating of the base form of an item, that presents in the form of bars, ingots, plates, wafers or other similar mass form, or coins.

When dealing in bullion, criminals may use third parties or facilitators to buy the gold or other precious metal on their behalf, distancing the criminals from the purchase and providing a level of protection for the asset against confiscation proceedings. They may also use a false identity or fraudulent identification in order to purchase the bullion without raising suspicion.

In regards to gold in particular, AUSTRAC reports that there are two key methods that can be used to launder money. One way is through the purchase of gold directly from a prospector with illicit funds. The prospector may be unaware of the purpose of the purchase or of any connections that the funds may have with organised crime. The criminals can then on-sell the gold to a legitimate business and declare their profits for the sale of the gold. The business may also be unaware that their purchase of the gold is part of a money-laundering process.

Another method is to launder money with gold is to use false invoices to conceal the transfer of funds. This can be done either through disguising the gold as another product or by stating that ‘gold’ is being traded when there is no gold, and it is simply a movement of money.
6.3.5 Debit cards

As highlighted earlier in this report, another channel that has been identified as being used to launder money is through the use of prepaid debit cards. An example of this in Australia was outlined by the Asia/Pacific Group on Money Laundering in its *Annual Typologies Report 2002–2003*. The report outlined that Travelex was issuing a debit card called a ‘cash passport card’ with a limit of $25,000. An Australian person with possession of one of these cards was loading it with funds just below the $10,000 reporting value. Another card linked to that account was posted overseas, where funds were being withdrawn through ATMs. The process was repeated, and more than $100,000 dollars was laundered in this manner.\(^4\)

The issuing of a debit card in the normal sense is providing a ‘designated service’; as such, the issuing body becomes a ‘reporting entity’ as defined under section 5 of the AML/CTF Act, and all the reporting requirements that come with being a reporting entity will apply.

Issuing ‘stored value cards’ are also designated services where:

- if whole or part of the card’s value can be withdrawn in cash, and the card is issued in an amount not less than $1,000, and
- if cash cannot be withdrawn from the stored value card, then the issuer will only be a designated service where the amount is not less than $5,000.

The issue with these debit cards, therefore, will be whether the transaction is suspicious enough to raise the concerns of the person issuing it, where the value of the card is not reportable in itself. Given that money launderers regularly use ‘mules’ to perform other tasks for them, it would be likely that they could use these persons to buy these cards for them as well, in values of less than $10,000, which they could then take overseas and withdraw.
6.3.6 Digital currencies

AUSTRAC identified in its 2012 Typologies and Case Studies report that digital currencies are a money-laundering risk due to the global reach of the Internet, the absence of face-to-face transactions, and the convenience of using electronic commerce. The extent and nature of money laundering through digital currencies is largely unknown, but the potential for exploitation is apparent. The money laundering risk for virtual currencies is that:

Digital currencies potentially allow individuals and entities to conduct quick and complex international funds transfers outside the regulatory requirements of the traditional financial system. Digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act.

Vulnerabilities of digital currencies include:

- the limited—or complete absence of—regulation, which creates difficulties for authorities to monitor criminal exploitation of those currencies
- the ability to convert and exchange one digital currency for another, providing 'layering' in the money-laundering cycle
- the ability to use illegally obtained currency to purchase digital currency
- the ability to convert virtual currency into 'real' currency by linking virtual accounts to a debit card.

The ACC reports that virtual currencies continue to be used to transfer value online, without relying on financial institutions to facilitate the transaction.

Media reports indicate that the major banks in Australia are closing accounts of digital currency providers, in response to tightening of rules around money laundering and terrorism financing.

Regulation of virtual currency is one issue being considered under the AML/CTF statutory review, as raised in the issues paper published as a guide to the review:

Market growth in internet-based and mobile services, along with the emergence of virtual currencies, raises questions about the need to include new designated services in the regime or whether it already provides the flexibility to capture these and other developments.

The use of digital currencies is also addressed in the section titled Internet and drugs, above.

6.3.7 Real estate and real estate agents as facilitators

Methods

The use of real estate as a money-laundering channel is well established in Australia. Some of the reasons why real estate is attractive to those wishing to launder proceeds of crime include:

- real estate can be bought in cash
- real estate provides an easy way to disguise the beneficial owner of the property
- real estate is a relatively stable investment
- real estate can be increased in value through renovations.

One way in which real estate is used to launder money is through the taking out of loans and mortgages. This method allows illicit funds to be disguised under the cover of a loan. A mortgage is taken out, and small repayments are then made with illicit funds. In some instances, a foreign company controlled by criminals may 'lend' back their own illicit funds to purchase property. Repayments are then made and the funds appear legitimate.
Another way in which money launderers use real estate to legitimise proceeds of crime is by having a third party act on their behalf in property transactions. This distances the criminal from the funds, makes it difficult to ascertain the beneficial owner of the property, and makes it more difficult for the property to be subject to confiscation orders.\(^5\) False employment and other supporting documentation may also be used to obtain loans from financial institutions.\(^6\) A further method used by criminals to distance themselves from the purchase of the property is to hold the property in the name of companies and trusts.\(^7\) These companies may be controlled by 'third parties', making the links to criminals and money laundering more difficult to detect.\(^8\) Those third parties may be real estate agents.

**Case study**

**Purchase of property by companies and third parties\(^59\)**

In Austrac’s 2010 Typologies and Case Studies report, an investigation into the laundering of funds stolen from multiple automatic teller machines (ATMs) was reported. In that instance, there were two suspects. The first suspect was employed to empty and replenish ATMs in Sydney. Five thefts occurred from ATMs in Sydney, amounting to approximately $714,000.

Shortly after these thefts, the second suspect, who was employed by a law enforcement agency, made a number of large cash deposits into the account of a company he owned. The second suspect also purchased a $60,000 boat, half of which was paid for in cash. The balance was paid for from a cheque drawn from the company account.

The second suspect also delivered $250,000 to an associate in Melbourne to purchase real estate. In addition, he also bought property in the name of one of his companies. The deposit and settlement payment were drawn from another one of his companies, which was not the business that had its name on the title.

Criminals can also use rental payments to hide illicit funds. They may purchase the property under the name of a third party and then rent the property from the apparent ‘owner’. This allows them to launder illicit funds by paying ‘rent’ on their own property, without it being known that they are the beneficial owner.\(^60\) They may also launder funds by renting the property to a third party, and then providing them with the funds to pay part or all of the rent.\(^61\) Alternatively, they may not rent the property out at all, but deposit fictitious rental income into an account.\(^62\)

Criminals can also manipulate property values and improve upon property to hide illicit funds. They can do this by under-valuing property, which means that they can use ‘legitimate’ funds to purchase the property. Any additional value is paid for ‘off the record’ with illicit funds.\(^63\) This also assists in reducing stamp duty.\(^64\) Criminals may also launder money through real estate by over-valuing the property to obtain a larger loan from the bank, which allows them to ‘pay back’ more, which legitimises a greater amount of illicit funds.\(^65\) Criminals can also make the funds difficult to trace by re-selling the property quickly at a higher value, usually to related third parties, companies or trusts.\(^66\) Criminals can also use illicit funds to pay for renovations on a property, which can then be sold at a higher price.\(^67\)
On-selling real estate to associates

AUSTRAC reported the facts of an investigation that saw a financial adviser laundering the proceeds of crime. It was alleged that the adviser was involved in a drug syndicate, and was using his business to launder the proceeds of drug crime. The suspect bought properties which he then obtained valuations for that exceeded the genuine value of the property. He then sold these properties at the higher valuation price to his associates. He used his company and industry contacts to facilitate the loan documents, many of which were falsified. On settlement date, the property settled simultaneously with another agreement entered into between the suspect and the associate. In the second agreement, the associate relinquished their interest in the property to the suspect. This method meant that, although the suspect had control over numerous properties, they did not appear on any government paperwork as an owner or person with an interest in the properties.

Investing in real estate is not only a method of money laundering for domestic criminals, but a way in which international crime groups can hide their assets from law enforcement authorities in their home country. The FATF’s April 2015 Mutual Evaluation Report considered that Australia’s risk factors include its attractiveness as a destination for foreign proceeds, ‘particularly corruption-related proceeds flowing into real estate, from the Asia-Pacific region.

The Mutual Evaluation Report states that foreign predicate offences are not frequently prosecuted from the money-laundering perspective in Australia, because foreign predicate offences are not considered major predicates for money laundering in Australia. ‘Authorities have referred to the difficulties of obtaining offshore evidence and have generally found the most successful way to obtain restraint or forfeiture orders is to seek registration of foreign orders.’ Further, federal and state action in Australia is not effectively coordinated in relation to the prosecution of money laundering of foreign predicate offences:

For example, while [money laundering] of foreign illicit proceeds through real estate is perceived to be a risk for Queensland (Gold Coast), Queensland has no [money-laundering] convictions for this activity. [The Australian Federal Police] indicated that it does not focus on this risk, believing this [money laundering] activity relates to State level predicates, whereas the Queensland Crime and Corruption Commission stated it does not focus on this risk as it relates to foreign money and is thus a matter for the [Australian Federal Police].

The FATF assessors did note ‘two examples of successful prosecution for foreign predicates (fraud and corruption) by the Australian Federal Police (AFP) and the registration of two restraint orders from Papua New Guinea in Queensland.’

Real estate agents

In each of the methods described above, real estate agents are necessarily part of the process and may facilitate money laundering either wittingly or unwittingly. Real estate agents are identified as ‘high risk’ in relation to money laundering but, despite that risk, remain unregulated by the AML/CTF Act.

The AUSTRAC strategic analysis brief on money laundering outlines the following services provided by real estate agents (and other ‘gatekeepers’ involved in real estate transactions) which may facilitate money laundering:

- establishing and maintaining domestic or offshore legal entity structures—for example, trusts or companies
- facilitating or conducting transactions on behalf of the criminal
• receiving and transferring large amounts of cash
• establishing complex loans and other credit arrangements
• introducing criminals to financial institutions
• facilitating the transfer of ownership of property to nominees or third parties.

The FATF Mutual Evaluation Report recommends that real estate agents be subject to obligations in the AML/CTF Act, along with lawyers and accountants.

There is currently some intersection with the AML/CTF Act, given that ‘real estate transactions most commonly go through a financial institution – for example, as loans, deposits or withdrawals.’ There reportable transactions intersect with the regulated sector, authorities have some visibility on potential money laundering through real estate. However, the FATF Mutual Evaluation Report suggests that more needs to be done, particularly given that real estate agents have been identified to be of high money-laundering risk in FATF’s national threat assessment of Australia.

The FATF Mutual Evaluation Report calls for regulation of real estate agents, given that they are one of the most exposed designated non-financial businesses and professions, stating that, ‘[o]f great concern is that Australia has not brought real estate agents within the AML/CTF regime.’ None of the designated services (described below, relating to lawyers and accountants) apply to real estate agents. See the Related activities section in this report’s Financial crimes chapter for recommendations on strengthening identity verification practices for the real estate industry in Queensland.

### 6.3.8 Professional facilitators

Professional facilitators are increasingly becoming involved, either knowingly or unwittingly, in organised crime. As organised crime entities realise they do not have the necessary skill set to undertake tasks associated with laundering the profits of their crime, they are turning to professional facilitators to assist them in these activities.

The ACC has noted that:

Professional facilitators perform a key role in money laundering associated with sophisticated financial crime. Serious and organised crime entities often require the services of a range of professionals to advise on, establish and, in some instances, administer complex financial and corporate structures that have been set up to launder proceeds of crime.

AUSTRAC reports that:

[Crime groups] use professionals, such as lawyers, accountants, financial advisers and real estate agents, to help undertake transactions to:

• obscure ultimate ownership through complex layers and structures
• conceal proceeds of crime
• legitimise illicit funds
• avoid tax
• avoid regulatory controls
• provide a veneer of legitimacy to criminal activity
• avoid detection and confiscation
• frustrate law enforcement investigations.
Organised criminal groups are turning to facilitators for two main reasons:

- they may lack the necessary skills, knowledge or access to carry out crimes, including sectors such as complex financial or computer based areas
- they use the facilitators to distance themselves from criminal activity and to give their activity the air of legitimacy.

This chapter focuses on lawyers, accountants and financial advisors as professional facilitators for organised crime groups laundering money. Real estate agents are also considered to be at high risk for facilitating money laundering, either knowingly or unwittingly, and are discussed above under the section titled, Real estate. Professional facilitators, and real estate agents, are not captured by the AML/CTF regime and consequently are not subject to reporting obligations or customer due diligence/know-your-customer requirements that are imposed on other entities.

Legal professionals and the facilitation of money laundering

The use of legal professionals as a form of professional facilitator to launder illicit funds is an established international money-laundering method. In 2013, the FATF concluded that criminals actively seek out the involvement of legal professionals in their money-laundering activities for four main reasons:

1. Expert legal advice is needed to devise complex schemes to launder vast amounts of money.
2. A legal professional is required to undertake the otherwise legitimate transactions, by virtue of a legal requirement or established practice—which in this instance involves the laundering of illicit funds.
3. The involvement of a legal professional lends respectability and credibility to transactions, dissuading suspicion and scrutiny from professionals and/or financial institutions.
4. The involvement of a legal professional further removes a criminal from the illicit funds, adding an additional hurdle to be overcome during an investigation by law enforcement.

AUSTRAC identifies five main methods through which a legal practitioner’s services may be targeted for money laundering or other criminal purposes. These methods largely align with the money laundering typologies set out by the FATF in their 2013 report on the vulnerabilities of the legal profession to money laundering. The five methods identified by AUSTRAC are:

1. use of legal practitioners to conduct transactions
2. use of legal practitioner’s trust or investment account
3. use of legal practitioners to recover fictitious debts
4. buying and selling real estate
5. establishing corporate structures.

Use of legal practitioners to conduct transactions

Criminals seeking to launder illicit funds may engage a legal professional to undertake transactions on their behalf in order to distance themselves from the transactions. In so doing, criminals seek to conceal the connection between themselves and the illicit proceeds. Legal practitioners may be complicitly or unwittingly involved in the laundering of illicit funds through their handling, deposit and transfer or withdrawal of illicit funds or the opening of bank accounts for criminal clients.

For example, financial institutions with comprehensive AML/CTF obligations may decide not to provide financing or bank accounts to individuals who pose a high risk of money laundering. In these circumstances, the individual may engage a legal professional to undertake these activities on their behalf, in order to avoid detection by the financial institutions.
Additionally, the FATF reports that criminals engage legal professionals to undertake their transactions due to their perception that legal professional privilege will delay, obstruct or even prevent effective investigation and prosecution by law enforcement.

**Use of legal practitioner’s trust or investment account**

Legal practitioners operate trust accounts to deposit, hold and disburse funds on behalf of clients. These accounts are attractive to criminals who seek to move their illicit funds through them in order to attract legitimacy and credibility to transactions which might otherwise appear suspicious.

A legal practitioner’s trust account can:

- be used as the first step in converting cash proceeds of crime into other less suspicious assets, such as property
- permit access to the financial system without the suspicion a criminal might otherwise attract
- serve to hide the ownership of criminally derived funds and assets
- be used as the link between other money-laundering processes such as the purchasing of real estate, the setting up of shell companies and the transferring of illicit funds.

### Case study

**Money laundering through a law firm’s trust account**

An individual is alleged to have fraudulently obtained $260,000 from a United Kingdom bank account and laundered the funds through an unwitting Australian law firm.

An employee of the firm received an email from a web-based email account, referencing a previous conversation with the law firm, where it was agreed that the firm would act on the individual’s behalf. The individual asked the employee to assist in the purchase of machinery in the UK by facilitating the transfer of $260,000 from the individual to a bank account in the UK.

Without undertaking reasonable identity checks, the firm’s trust account details were provided and the employee confirmed that the firm would act in the matter.

After the $260,000 was transferred to the firm’s trust account, the individual requested that the money be transferred to another bank account in the UK after costs and transfer fees were deducted. The employee subsequently completed the transfer to the designated account, facilitating the laundering of the allegedly stolen funds.

Another method used to launder funds through legal professionals’ trust accounts is through aborted transactions. The criminal will engage a legal professional for the alleged purpose of completing a legitimate transaction—such as the purchase of property—and transfer money to the legal professional’s trust account for this purpose. The alleged transaction, for one reason or another, will then collapse before completion. The criminal then asks for the money to be returned or paid to one or more third parties. The aborting of transactions is not an infrequent occurrence, and as a result, legal practitioners may find it difficult to distinguish between legitimate transactions and those intended to launder funds.
6 Money laundering

Case study

Solicitor launders client funds through trust account

In 2011, a solicitor in the UK was struck off the roll for acting in a number of property transactions which were suspected to be undertaken to launder money. The solicitor received instructions from an individual to purchase property on behalf of other clients who provided funds for the purchase. These funds were deposited, prior to the purchase, into the client trust account. The transaction was then cancelled on the same day that the funds were received, and a request was provided, directing that the funds be transferred to a third party.

A legal professional’s trust account is, therefore, very attractive to criminals seeking to launder illicit funds, as it works to disguise the criminal origin of such funds.

Use of legal practitioners to recover fictitious debts

An area of concern in Australia is the use of legal practitioners in schemes designed to mimic ‘debt’ recovery. Criminals seeking to launder money in this manner engage legal practitioners to move illicit funds through the practitioner’s trust account by disguising the funds as being the proceeds of a legitimate debt recovery action. AUSTRAC identifies two variations of this method:

Method A
1. A foreign company requests the debt recovery services of an Australia-based legal practitioner.
2. The foreign company (the client) may offer to pay legal fees above standard rates.
3. The legal practitioner performs little, if any, debt recovery work on behalf of the client. Instead, the legal firm quickly receives substantial amounts of money from supposed debtors (either in Australia or overseas).
4. The legal practitioner advises the client when the funds have been received and sends the funds to the client’s account or a third-party account.

Method B
1. The business creates false invoices to provide a façade of debts owing.
2. A legal practitioner is engaged for debt recovery services.
3. Debtor payments (which are actually illicit funds) are paid to the legal practitioner and subsequently returned to the client.

The end result of both methods is the same: Illicit funds have been disguised as outstanding debts, and by moving through the legal practitioner’s trust account, have returned to the client as apparently legitimately derived funds.

Buying and selling real estate

Legal practitioners are often involved as a matter of practice in the buying and selling of real estate. Real estate is, however, a common outlet for criminal proceeds, as it is generally an appreciating asset. The sale of the asset can therefore provide a legitimate reason for the appearance of funds. Criminals also require places to live and from which to conduct their business activities, making real estate investment an attractive option.
Legal practitioners may knowingly or unwittingly assist criminals in laundering money through real estate by:  
- establishing and maintaining domestic or foreign legal structures such as trusts or companies, which help obscure ownership, hide the source of the funds, and frustrate law enforcement  
- facilitating or conducting financial transactions—for example, back-to-back sales, where quick successive sales of property allow criminals to inflate the value of the property, allowing illicit funds to be injected into the transaction  
- receiving and transferring large amounts of cash, allowing illicit funds to enter the market  
- falsifying documents—for example, buying real estate in a false name  
- establishing complex loans and other financial arrangements  
- facilitating the transfer of ownership of property to nominees and third parties.

**Establish corporate structures**

Legal practitioners have the specialist skills and knowledge to establish and administer corporate and trust structures. Criminals can use layers of companies and trusts in different jurisdictions in order to retain control over criminally derived assets whilst frustrating law enforcement investigations into the ownership of the assets. The distance between criminals and their illegal activities provided by corporate structures greatly assists in the laundering of illicit funds.

Criminal networks will use a legal practitioner to establish a corporate network, through which they will invest and buy in high-value goods such as real estate. This allows the criminals to reinvest illicit funds into the legitimate economy, concealing the proceeds of crime and effecting the money-laundering process.

There are numerous methods by which criminals can use corporate structures to this effect, often involving complex corporate structures spread across multiple foreign jurisdictions, usually with at least one jurisdiction having strict secrecy provisions.

**Accountants and financial advisers**

AUSTRAC has published strategic analysis documents specific to legal practitioners and the real estate industry. No similar document analyses the role of accountants or financial advisers in money laundering. However, some of the services provided by lawyers described above may also be provided by accountants and financial advisers—particularly the establishing of corporate structures. It is, therefore, expected that where such services are provided by accountants or financial advisors, the same vulnerabilities are present as those outlined above under lawyers.

The Commission received information that accountants may be utilised in setting up a business structure. Accountants and financial advisers may assist organised crime by providing financial advice, preparing trust documentation, preparing loan and property development documentation.

The following case studies demonstrate how accountants may facilitate money laundering:

**Case study**

**Real estate and trust accounts used to launder cannabis cash**

An Australian drug syndicate used multiple money-laundering methods to launder more than $1 million worth of proceeds of crime. Trust accounts, a ‘front’ company, high-value goods and real estate were used to launder the profits from cannabis sales. The syndicate also misused the services of two ‘professional facilitators’ (an accountant and solicitor) to facilitate its criminal activity.
The syndicate created trust accounts and investment companies. It gave an accountant $100,000 cash from the proceeds of cannabis sales, and instructed the accountant to purchase shares in the name of the trust accounts and investment companies.

One syndicate member purchased a property worth more than $700,000 in a family member’s name. The property purchase was financed using a mortgage. This is an example of a criminal purchasing high-value goods in the name of a third party to disguise the true ownership of assets. Over a two-month period, the syndicate member paid more than $320,000 in 16 cash deposits to their solicitor (who provided conveyancing services and acted on behalf of the syndicate member in the transaction) to pay off the mortgage on the property. These cash payments were the proceeds of crime.

In relation to tax crime, professional facilitators are an organised crime risk, with:

[Cr]iminally complicit tax agents who engage in taxation fraud able to cause particular harm because of their expert knowledge of the taxation system, the taxation information they possess, and the level of access that they have to online services provided by the [Australian Taxation Office].

Tax advisors are commonly accountants, but may also be tax lawyers or be qualified to practice in both professions. Money laundering related to tax crime may therefore be facilitated by either accountants or lawyers.

A number of accountants have been prosecuted in Australia for their involvement in tax evasion schemes. One case (R v de Figueiredo) is discussed in the section on Related activities in the Financial crimes chapter.

Project Wickenby—a joint taskforce involving the Australian Taxation Office, AFP, ACC, Australian Securities and Investments Commission, ASTRAC and the CDPP—was established in 2006 with the purpose of preventing people from promoting or participating in tax avoidance and evasion schemes. The Serious Financial Crime Taskforce (which commenced on 1 July 2015) will build on Project Wickenby’s success. Project Wickenby claims to have raised over $2.2 billion in tax liabilities and improved compliance behaviour following high-profile investigations, prosecutions and sentencings.

The FATF’s national threat assessment on money laundering identified illicit narcotics and tax frauds (and other frauds) as the major predicate crimes for money laundering. Thus, accountants and financial advisors involved in illegal tax avoidance or tax evasion schemes are, by extension, often involved in laundering money otherwise payable to the Australian Taxation Office. The following case example from New South Wales highlights the link between money laundering and tax evasion.

**Case study**

*R v Jones; R v Hili*

Hili and Jones were builders who participated in a tax evasion scheme promoted by their Sydney-based accountants and a Vanuatu-based accountant. Hill and Jones were both charged with obtaining a financial advantage by deception under section 134.2 of the Criminal Code (Cth). Jones was also charged with defrauding the Commonwealth under section 29D of the Crimes Act (Cth) and with intentionally dealing in an instrument of crime, namely money or property worth $100,000 or more, under section 400.4(1) of the Criminal Code (Cth).

Without detailing the elaborate round robin scheme which facilitated the tax evasion, the money-laundering charge arose out of four telegraphic transfers (totaling over $130,000) over about 12 months, which Jones had caused his company to make. He was the sole director and share-holder of that
company. ‘Each payment was the initial step in the implementation of the international round robin scheme relating to that payment.’

The Crown appealed the sentences imposed at first instance (18 months imprisonment with a recognisance release order after seven months). The Court of Criminal Appeal allowed the appeal in part, set aside the sentences and imposed the following sentences in lieu: three years (Hili) and two and a half years (Jones).

The accountant who promoted the scheme was convicted separately of conspiring to defraud the Commonwealth and was sentenced to eight years and 11 months imprisonment.

In obiter, Rothman J (with whom McLellan CJ and Howie J agreed) stated that serious issues were raised relating to double jeopardy in charging the money-laundering offence over and above the criminal offence from which the money was necessarily derived, an issue also raised in Nahlous v R and Thorn v R. The criticism of this practice was noted in the FATF Mutual Evaluation Report, to some extent addressed by a CDPP litigation direction to prosecutors that the charging of a predicate offence and a money laundering offence ‘will not be an abuse of process where it is necessary to charge both offences to reflect the overall criminality in the case.’

In subsequent appeals to the High Court, no issue was raised in respect of the comments made by the New South Wales Court of Criminal Appeal in respect of the charge of money laundering. Both Hili and Jones sought special leave to appeal against the increased sentences imposed. Special leave was granted by the High Court but the appeals were dismissed.

See the Related activities section in the Financial crimes chapter for discussion of the ethical obligations of accountants and their self-regulatory regime.

Reporting obligations of professionals in Australia

Financial Transaction Reports Act 1988 (Cth)

Under section 15A of the Financial Transaction Reports Act 1988, solicitors, solicitor corporations and partnerships of solicitors must provide a significant cash transaction report to AUSTRAC if a significant cash transaction is entered into by or on their behalf. A ‘significant cash transaction’ is defined in section 3 of the Act as ‘a cash transaction involving the transfer of currency of not less than $10,000 in value.’

The significant cash transaction report must be lodged within 15 days after the end of the day on which the transaction occurred when it concerns the transfer of Australian currency. If the significant cash transaction involved foreign currency, then the report must be made by the end of the day after the transaction took place.

Those obligations do not apply to accountants or financial advisers.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Additional reporting obligations apply to legal professionals, as well as to accountants and financial advisers, if they are involved in the provision of a designated service under the AML/CTF Act. Designated services are set out in section 6 of the AML/CTF Act and involve a wide range of businesses activities.

Services provided by legal professionals that may constitute designated services include loans (Item 6 & 7 of Table 1) or the provision of certain services as the holder of an Australian Financial Services Licence (License) (Item 54 of Table 1). The latter also applies to financial advisers and accountants who provide services as a License holder.

License holders ‘authorised to carry out broker-type activities as agents for another person to acquire and dispose of securities’ will be providing a designated service (Item 33 of Table 1). If accounting or financial service companies carry on the business of issuing or selling interests in a managed investment scheme, they will be providing a ‘designated service’ (Item 35 of Table 1).
Professionals who provide a designated service under the AML/CLF Act must report to AUSTRAC:

- threshold transactions
- suspicious matters

**FATF Mutual Evaluation Report 2015 and professional facilitators**

In April 2015 the FATF published its *Anti-money laundering and counter terrorism financing measures Australia: Mutual Evaluation Report*. A number of recommendations were made concerning the improvement of Australia’s current AML/CTF measures.

Priority actions were itemised, including:

- Ensure that lawyers, accountants, real estate agents, precious stones dealers, and TCSPs (trust and company service providers) understand their money laundering and terrorist financing risks, and are required to effectively implement AML/CTF obligations and risk mitigating measures in line with the FATF Standards.\(^{130}\)

With regards to legal professionals and accountants, the *Mutual Evaluation Report* identified a single key area of concern, namely that legal professionals are only subject to the AML/CTF Act when providing a designated service.\(^{131}\)

The *Mutual Evaluation Report* states that professional facilitators (legal professionals, accountants and trust and company service providers) are universally understood to be a major money-laundering risk.\(^{132}\) Australia’s own National Threat Assessment identifies professionals, such as lawyers and accountants, as facilitating the establishment of legal structures and advice to facilitate money laundering of organised crime groups.\(^{133}\) Despite this high risk, legal professionals, accountants and financial advisors in Australia are only subject to the comprehensive reporting obligations of the AML/CTF Act when providing a client with a designated service. As this only encompasses a small component of legal and accounting practice, the majority of those professionals in their day-to-day practice are not subject to the AML/CTF Act requirements.

This means that professionals are not required to report suspicious and threshold transactions to AUSTRAC unless providing a designated service. Those professionals, along with real estate agents, are also not required to implement AML/CTF programs to mitigate money laundering and counter terrorism financing. This would appear to be at odds with the risk-based approach prescribed by the FATF recommendation.\(^{134}\)

The *Mutual Evaluation Report* found that designated non-financial businesses and professions not subject to the requirements under the AML/CTF regime generally demonstrated a poor understanding of money laundering and terrorist financing risks.\(^{135}\) In relation specifically to legal professionals, the FATF asserts that the inapplicability of the AML/CTF Act is particularly problematic, given the role that legal professionals play in the registration of corporate structures, which, as detailed above, are a key tool for the laundering of illicit funds.\(^{136}\) The *Mutual Evaluation Report* states that 80 to 95 per cent of companies registered with the Australian Securities and Investments Commission were registered online by a third party, including legal professionals.\(^{137}\)

The FATF states that the limited application of the AML/CTF Act to legal professionals is in direct contrast to the high threat assessment in the National Threat Assessment.\(^{138}\) The *Mutual Evaluation Report* therefore recommends extending the AML/CTF Act obligations to legal professionals, in order to bring legal professional AML/CTF obligations in line with the FATF Standards.\(^{139}\)

**Evidence of professionals in Queensland being involved in money laundering**

The Commission required the QPS, the CCC, the Queensland Law Society, the Bar Association of Queensland and the Legal Services Commission to provide any information in their possession from the last three years which suggested or tended to suggest that solicitors and/or barristers were either directly or indirectly involved in the laundering of monies obtained from the commission of offences.
As detailed in the Financial crimes chapter of this report, while there were two matters considered to be relevant to this particular area, they are currently subject to judicial proceedings and therefore the Commission cannot have regard to them, in accordance with the Terms of Reference.

The Commission also required the QPS and the CCC to provide any information in their possession from the last three years which suggested or tended to suggest that accountants or financial advisors were either directly or indirectly involved in the facilitation of organised crime. The Commission received information suggesting that accountants may be knowingly or unwittingly involved in organised crime and the facilitation of money laundering, but there were no matters to which the Commission could have regard.

The Commission is aware that an accountant on the Gold Coast has recently been charged with money laundering, but as the matter is subject to judicial proceedings the Commission may not have regard to it.

The Commission also requested information from each of the three professional accounting bodies (Institute of Charted Accountants Australia, CPA Australia and the Institute of Public Accountants). The Commission received no information from those bodies indicating they were aware of any involvement of their members in organised crime.

(Endnotes)


8 [2007] QCA 396

9 R v Columbus [2007] QCA 396 at [19].


20 [2013] VSCA 40


33 [2015] NSCCCA 95


Money laundering

Queensland Organised Crime Commission of Inquiry

6 Money laundering


<table>
<thead>
<tr>
<th>Number</th>
<th>Source</th>
<th>Location</th>
</tr>
</thead>
</table>
6 Money laundering


113 Statutory Declaration of Ross Barnett, 10 June 2015, para 9.


116 [2013] QCA 303


119 [2010] NSWCCA 108


122 [2010] NSW CCA 58

123 [2009] NSW CCA 294


125 (2010) 242 CLR 520

126 Section 3, Financial Transaction Reports Act 1988 (Cth).

127 Section 3, Financial Transaction Reports Act 1988 (Cth).


6.4 Statutory review of Anti-Money Laundering and Counter Terrorism Financing Act

The Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) is currently the subject of statutory review by the Attorney-General’s Department of the Commonwealth Government. Submissions to this review closed in March 2014 and there were further round table discussions with key stakeholders in 2014 and 2015. The Department has advised that relevant findings of the FATF Mutual Evaluation Report will be taken into account in the review and will be reflected in the recommendations made to the Commonwealth Government.

Given that the second tranche of legislation relating to designated non-financial businesses and professions is still yet to be enacted, it is hoped that the Commonwealth Government will amend the AML/CTF Act to cover these professions in the legislation, following the review.

6.5 Conclusion

Money laundering to ‘clean’ illicit funds is a significant global issue. Australia is one of the largest financial markets in the Asia-Pacific region, which makes it very susceptible to money laundering. In Queensland, the requirement to obtain the consent of the Attorney-General prior to a person being charged with the Queensland offence of money laundering under the Criminal Proceeds Confiscation Act 2002 (Qld) is an issue that should be addressed immediately. The practical effect of the consent requirement is that the QPS is electing to charge people with the Commonwealth offence over the Queensland offence. The Commission can see no reasonable rationale for the requirement for ministerial consent, and its omission is supported...
by the Queensland Police Service, the Crime and Corruption Commission and the Acting Director of Public Prosecutions.

At a Commonwealth level, the international authorities have been clear in their views that Australia should implement the remaining recommendations of the FATF. The Australian Government has been promising the implementation of the second tranche of the AML/CTF Act for a considerable period of time. Given that the Act is now subject to a statutory review, it would seem that this issue is being considered by the relevant authorities. It would be hoped that additional legislative requirements will be implemented in the near future, to capture those designated non-financial businesses and professions who are clear targets for money laundering throughout the country and the world.

(Endnotes)

7.1 Introduction

In investigating the extent and nature of organised crime in Queensland, the Commission was required by the Terms of Reference to consider and report on the relationship between organised crime and corruption in this state\(^1\). In the context of this Inquiry, the Commission interpreted that requirement as referring to public sector corruption—an issue that is the subject of much analysis and focus by law enforcement and academics around the world when considering activities and links to organised crime.

The issue of public sector corruption concerns organised crime groups forming—or attempting to form—corrupt relationships with public officials in order to obtain information that minimises the risk of detection and prosecution.\(^2\) Prior research has found a strong association between public sector corruption and organised crime groups.\(^3\) The Australian Commission for Law Enforcement Integrity advised the Commission that corruption-enabled border crime is an ongoing threat to law enforcement integrity in Australia.\(^4\)

The Australian Institute of Criminology has reported that little research has been conducted in Australia regarding any links between organised crime and corrupt public officials. While there have been some highly publicised instances of official corruption with links to organised crime groups, compared to the international community, the instances are low in Australia. Additionally, there is 'little public source evidence to suggest that there is any large-scale infiltration of the public sector by criminal organisations'.\(^5\)

In fact, the Transparency International's 2014 Corruption Perceptions Index ranked Australia the eleventh-cleanest country in public perceptions of corruption. The Corruption Perceptions Index ranks countries and territories based on how corrupt their public sector is perceived to be, based on expert opinion. The 2014 Index ranked 175 countries.

The Australian Crime Commission (ACC) asserts that Australia’s positive ranking does not mean that corruption is absent in Australia, and, moreover, that ‘organised crime continually probes for weaknesses in systems and will take advantage of any opportunities to corrupt public officials.’\(^6\)

The Australian Institute of Criminology notes the attention that organised crime has received from legislatures and law enforcement agencies in Australia during the last decade, and observes that enhanced legislation and law enforcement approaches create a risk of ‘tactical crime displacement’. Tactical crime displacement refers to criminals modifying their tactics in order to circumvent the effects of new legislation or increased law enforcement activity. One particular risk of tactical crime displacement is the potential for organised crime groups to focus more on forming corrupt relationships with public officials.\(^7\)
7.2 Position in Queensland

It is the experience of the Crime and Corruption Commission (CCC) that in Queensland, after the Fitzgerald Inquiry era, corruption of public officials is usually opportunistic rather than endemic. Further, the CCC has not found evidence to suggest that organised crime entities are attempting to proactively infiltrate government departments or agencies for the purpose of furthering criminal activity. 8

The CCC advised that, after the Fitzgerald Inquiry era, it continues to investigate allegations of police officers and public servants protecting the activities of criminals—such protection usually being by way of the release of confidential information from police databases or in relation to operational activity. However, the majority of these investigations involve criminal activity that does not involve persons who have connections with organised criminal networks. 9

Nevertheless, the CCC acknowledges that, while there is no evidence in Queensland of a significant corruption problem, such lack of evidence does not necessarily suggest that this type of conduct is not a real risk to government. 10 In its view, the areas of risk are law enforcement agencies, as well as public sector agencies that control or regulate industries or activities, and such agencies that issue identification documents. Further, the CCC believes that any government agencies that have access to or relate to the following functions are at risk of being targeted by organised crime: 11

- databases (personal and business data and other official documents)
- controlled goods (pharmaceuticals, hazardous compounds, arms, ammunition, and explosives)
- licensing and accreditation processes (transport, security, liquor, gaming, prostitution, tattoo parlours)
- operational intelligence (police, corrections, security [IT, alarm, and CCTV systems], freight movement)
- financial transactions
- uncontrolled goods (any attractive item liable to ordinary theft).

The CCC stated that factors that might enable organised crime to corrupt public officials include poor supervision, deficiencies in agencies’ internal control mechanisms, inadequate pre-employment inquiries, new technologies, improper associations between officials and relatives or friends, and, in the case of the Queensland Police Service (QPS), the absence of a directed transfer policy. The absence of a directed transfer policy enables police officers to stay in a single region long-term—a particular and long-standing issue on the Gold Coast. 12

The widespread use of social media is considered to be a factor raising the risk of corrupt relationships developing. The Australian Commission for Law Enforcement Integrity has identified that the use of social media by law enforcement officers may leave some vulnerable to corrupt overtures. It suggests that law enforcement officers need to be circumspect about their professional affiliations when using social media. Indeed, the same observation could be made about all public officials. 13

The Australian Institute of Criminology observed that the significant amount of personal and sensitive information found on social networking sites can assist criminals to undertake more refined research on targets, allowing for comprehensive dossiers to be developed. 14

The Australian Institute of Criminology also identified the emerging risk of the use of information and communications technologies by organised crime groups to assist in the corruption of public officials. Organised crime groups use such technologies to unlawfully access personal information of public servants, enhancing their ability to coerce individuals into behaving corruptly. 15

7.3 Addressing the risk of corruption

Queensland has in place a wide range of legislative measures aimed at guarding against corruption in the public sector.
Offences

Chapters 12 and 13 of Queensland’s Criminal Code contain a range of offences concerning corrupt conduct by public officials. These offences attract substantial maximum penalties of imprisonment.

Section 85 of the Criminal Code contains the offence of disclosing official secrets. A person who is or has been employed as a public officer, who unlawfully publishes or communicates confidential information, commits an indictable offence punishable by a maximum penalty of two years imprisonment.

Section 86 of the Criminal Code contains the specific offence of obtaining or disclosing confidential information about the identity of a criminal organisation informant (such phrase is defined within the section). The offence carries a maximum penalty of 10 years imprisonment.

Chapter 13 of the Criminal Code contains offences addressing corruption and abuse of office. The offence of official corruption (section 87) carries a maximum penalty of seven years imprisonment, or 14 years if the offence is committed by or in relation to a Minister of the Crown. Official corruption is concerned with public officers corruptly seeking or receiving any benefit on account of conduct concerning the discharge of the public officer’s duties. The offence also applies to those persons who corrupt or seek to corrupt the public officer. The offence is limited in its application, because it is concerned with the public officer’s duties of office.

Section 92A of the Criminal Code provides the broad-ranging offence of misconduct in relation to public office. This offence extends beyond a public officer’s duties, and applies to misconduct in general. The offence applies to a public officer who, with intent to dishonestly gain a benefit for themselves or another person (or cause a detriment to another person), deals with information gained, performs or fails to performs a function of their office, or acts in abuse of the authority of their office. The offence carries a maximum penalty of seven years imprisonment, increasing to 14 years if the person who gained a benefit from the offence was a participant in a criminal organisation.

Role of the Crime and Corruption Commission

One of the main purposes of the CCC is to investigate cases of corrupt conduct, especially the more-serious cases in units of public administration. Units of public administration include the Public Service, the Queensland Police Service (QPS), local government, and corporate entities such as universities established by the State.

The expression ‘corrupt conduct’ is broadly defined in the Crime and Corruption Act 2001 to mean:

... conduct of a person ... that –

(a) adversely affects, or could adversely affect ... the performance of functions or the exercise of powers of –

(i) a unit of public administration; or

(ii) a person holding an appointment; and

(b) results, or could result ... in the performance of functions or the exercise of powers ... in a way that –

(i) is not honest or impartial; or

(ii) involves a breach of trust placed in a person holding an appointment, either knowingly or recklessly; or

(iii) involves a misuse of information or material acquired in or in connection with the performance of functions or the exercise of powers of a person holding an appointment; and
(c) is engaged in for the purpose of providing a benefit to the person or another person or causing a detriment to another person; and

(d) would, if proved, be –

(i) a criminal offence; or

(ii) a disciplinary breach providing reasonable grounds for terminating the person’s services, if the person is or were the holder of an appointment.

If a public official reasonably suspects that a complaint, information or matter involves or may involve corrupt conduct, then that official is bound to notify the CCC of the complaint. The CCC must ensure that any such complaint, information or matter is dealt with in the appropriate way. The CCC may investigate cases itself, or refer complaints to an appropriate body to investigate. The CCC is required to focus on the more-serious cases of corrupt conduct and cases of systemic corrupt conduct. The CCC has an extensive range of powers available to it to conduct any such investigations.

If the CCC investigates and decides that prosecution proceedings are warranted, or that disciplinary action should be considered, then it may report on the investigation to the appropriate prosecution agency for the purpose of prosecution proceedings. Or, it may report to the relevant chief executive of the unit of public administration for the purpose of disciplinary proceedings being commenced by the chief executive. Additionally, the CCC may apply to the Queensland Civil and Administrative Tribunal (QCAT) for it to hear and decide an allegation of corrupt conduct in some cases.

Under the Public Service Act 2008, public service managers are to take all reasonable steps to ensure that all officers under their supervision are aware of what constitutes corrupt conduct under the Crime and Corruption Act.

Role of public service agencies

All public service officers must provide impartial advice to Government; discharge their duties impartially and with integrity; act honestly, fairly and in the public interest; and otherwise act ethically. Public service officers who are guilty of misconduct (inappropriate or improper conduct in an official capacity, or inappropriate or improper conduct in a private capacity that reflects seriously and adversely on the public service), or who breach standards of conduct made under codes of conduct, can be liable to disciplinary action—including the sanction of dismissal from the public service. Departments’ handling of allegations of misconduct can be reviewed by the Public Service Commission.

The Public Sector Ethics Act 1994 requires public officials to comply with standards of conduct stated in the code of conduct applicable to the particular official. Chief executive officers must ensure that all public officials receive education and training about ethical behaviour upon appointment and at regular intervals during the course of their employment. Public officers who contravene a code of conduct or standard of practice face disciplinary action under the Public Service Act 2008 or other relevant legislation or disciplinary processes.

Under the Police Service Administration Act 1990, police officers are obliged to report suspected misconduct. Police officers are liable to disciplinary action if their conduct is found to constitute misconduct or a breach of discipline. The expression ‘misconduct’ means conduct that is disgraceful, improper or unbecoming an officer, shows unfitness to continue as an officer, or does not meet the standard of conduct the community reasonably expects of a police officer.

Recovery of superannuation

A publicly funded superannuant who is convicted of an offence, such as official corruption committed while holding public office, is liable to pay to the state the amount contributed by the State to his or her superannuation. The Public Officers Superannuation Benefits Recovery Act 1988 provides the legislative regime for recovery.
In a submission to the Commission, the CCC said that it should be the agency to initiate recovery action under the Public Officers Superannuation Benefits Recovery Act. The CCC pointed out that matters suitable for recovery under the Act will, in most cases, have arisen as a result of investigations conducted by the CCC. Currently, recovery action is undertaken on the State’s behalf by Crown Law. The Crown Solicitor advised that, since 1988, only 32 matters had been referred to Crown Law for recovery action. The Crown Solicitor did not consider there to be any advantage to be achieved by transferring responsibility for recovery to the CCC.

Other strategies and measures

There are strategies and measures that relevant agencies can implement to lessen corruption risks.

The CCC identified the following:

- the implementation of declarable associations policies
- investment in data-mining to enable agencies to proactively identify and manage inappropriate associations
- well-considered recruitment strategies, including stringent vetting processes
- strong internal control mechanisms and practices, particularly around sensitive work practices
- a directed transfer policy in relation to the QPS
- ‘zero-tolerance’ policies, supported by severe penalties for staff who knowingly assist criminals, either directly or by inaction, in corrupting officials or official processes
- timely exchange of information between law enforcement agencies.

Declarable associations

Declarable associations policies aim to minimise the risk presented by public officers who fail to identify and properly manage those associations that have the potential to impact on the reputation or integrity of the officer, and consequently affect the relevant agency and its activities.

The QPS has implemented a mandatory declarable associations policy.

While chief executives of government departments, senior executive service officers, and public service employees are required to fully disclose a conflict of interest that may have a bearing or be perceived to have a bearing on their ability to impartially discharge their duties of office, the CCC is of the view—and the Commission agrees—that declarable associations policies should be implemented.19 It is the Commission’s view that such mandatory declaration policies will increase awareness across the Queensland public sector of the risk posed to public officers of being targeted and groomed by organised crime groups.

Recommendation

7.1  The Commission recommends that all Queensland Government departments and agencies undertake an audit to identify high-risk areas, in terms of information, assets, materials and functions.

Persons employed in those identified high-risk areas complete (and keep current) a statement of their declarable associations.

The Commission also acknowledges the CCC’s further proposal for mandatory staff rotations in identified high-risk roles and within identified agencies, to ensure professional distance in the oversight/client relationship, and to minimise risks inherent in familiarity, territorial claims and habitual use of government assets.20 The proposal is worthy of investigation and consideration.
7.4 Conclusions

The issue of public sector corruption concerns organised crime groups forming or attempting to form corrupt relationships with public officials, in order to obtain information that minimises the risk of detection and prosecution.\(^{21}\)

It is the experience of the CCC that in Queensland, following the Fitzgerald Inquiry era, corruption of public officials is usually opportunistic rather than endemic. Further, the CCC has not found evidence to suggest that organised crime entities are attempting to proactively infiltrate government departments or agencies for the purpose of furthering criminal activity.\(^{22}\)

The Commission did not discover any evidence of—or receive any reliable information to suggest—corruption of public officials by persons associated with organised crime. Some informants asserted that such links might exist, but the foundations for the assertions were largely personal beliefs that such links exist, rather than evidence or reliable information that they did in fact exist.

While there is no evidence in Queensland of a significant corruption problem, common sense dictates that the potential for such conduct is a risk to government, and that proactive measures should be taken to minimise such risks. The focus should be on law enforcement agencies, and public sector agencies that control or regulate industries or activities, and which issue identification documents.

The CCC stated that factors that might enable organised crime to corrupt public officials include poor supervision, deficiencies in agencies’ internal control mechanisms, inadequate pre-employment inquiries, new technologies, improper associations between officials and relatives or friends, and—in the case of the QPS—the absence of a directed transfer policy.

The Commission recommends the introduction of mandatory declarable associations policies in identified high-risk agencies or high-risk business units within agencies. It is the Commission’s view that such mandatory declaration policies will increase awareness across the Queensland public sector of the risk posed to public officers of being targeted and groomed by organised crime groups.

(Endnotes)

1 Commissions of Inquiry Order (No 1), para 3(b).


4 Submission of Australian Commission for Law Enforcement Integrity, 7 July 2015, p. 5.


17 Section 26(2)(c) Public Service Act 2008.

18 Section 26(1) Public Service Act 2008.

19 Submission of Crime and Corruption Commission, 22 May 2015, p. 27.

20 Submission of Crime and Corruption Commission, 22 May 2015, p. 27


8.1 Introduction

The Commission was required to investigate and evaluate the adequacy of current legislation and resources available to law enforcement, intelligence, and prosecution agencies to effectively address organised criminal activity, including the recovery of the proceeds of crime.¹

As outlined in the introductory chapter of this report, the Commission’s approach to the 2013 suite of legislation introduced by the Newman Government to combat organised crime, particularly that of outlaw motorcycle gangs, was to have regard to the laws but not examine their adequacy, given that the Queensland Taskforce on organised crime legislation was specifically established to review those laws. The Commission noted the Queensland Government’s intention, as evidenced in the Terms of Reference for the Taskforce, to repeal and replace the 2013 laws or to substantially amend them.

The Commission also notes the Criminal Organisation Act 2009. The Criminal Organisation Act has had little use, will expire on 15 April 2017,² and must be reviewed this year to establish whether the Act is operating effectively and meeting its objects.³ Given that the Criminal Organisation Act is subject to a mandatory review this year to establish its effectiveness, the Commission has noted the Act but has not further examined it.

While the issue of the adequacy of current legislation is addressed throughout this report in relevant chapters, an issue that arose for specific consideration was whether a new offence dealing with organised criminal activity should be added to the Criminal Code.

With regards to the recovery of the proceeds of crime, the main issue that arose for consideration was whether the Office of the Director of Public Prosecutions (ODPP) should continue to perform functions under the Criminal Proceeds Confiscation Act 2002.

8.2 Organised crime specific offence

8.2.1 Queensland

A possible rationale for an organised crime offence has been identified in the following Canadian case:

Working collectively rather than alone carries with it advantages to criminals who form or join organized groups of like-minded felons. Organized criminal...
entities thrive and expand their reach by developing specializations and dividing labour accordingly; fostering trust and loyalty within the organization; sharing customers, financial resources, and insider knowledge; and, in some circumstances, developing a reputation for violence. A group that operates with even a minimal degree of organization over a period of time is bound to capitalize on these advantages and acquire a level of sophistication and expertise that poses an enhanced threat to the surrounding community. (R v Venneri [2012] 2 SCR 211 at [36]).

There is no offence in Queensland’s Criminal Code directed at proscribing acts or omissions designed to further the interests or objectives of a criminal group. The Vicious Lawless Association Disestablishment Act 2013 provides a mandatory sentencing regime for persons convicted of prescribed offences and held to have committed the offence for the purposes of, or in the course of participating in, the affairs of an association.

In a submission to the Commission, the Queensland Law Society stated that it did not support the creation of a new offence of organised crime, because the Criminal Code contains offences that would cover such conduct.4

The Criminal Code contains a number of conspiracy offences.5 A conspiracy involves an agreement between two or more persons to carry out an unlawful purpose or to do a lawful act by unlawful means. So the conspiracy offences can catch members of organised criminal groups who agree to commit offences, but they do not represent a legislative response that is specific to the activities of organised criminal groups.

Nevertheless, the Criminal Code does not confine criminal liability for an offence to the person who actually does the act or makes the omission which constitutes the offence. Section 7 of the Code extends liability to the following persons:

- Persons who do or omit to do acts for the purpose of enabling another person to commit an offence can be liable for the offence.
- Persons who aid another person to commit an offence can be liable for the offence.
- Persons who counsel or procure another person to commit the offence can be liable for the offence.

The Criminal Code (section 8) also extends criminal liability in cases of unintended offences in the following way: When two or more persons form a common intention to carry out an unlawful purpose together, and in furtherance of that purpose another offence is committed, each of them will be liable for that other offence if it was a probable consequence of the carrying out of the purpose agreed. In other words, even if the offence actually committed was not the offence intended but was merely one that could well have resulted from the carrying out of the agreed purpose, those who made the agreement can be criminally liable. Persons who counsel others to commit an offence are liable for the offence actually committed—even if that offence was not the offence counselled—if the facts constituting the offence actually committed were a probable consequence of acting upon the counsel.6

When consulted by the Commission, the then Director of Public Prosecutions, Mr AW Moynihan QC, expressed the view that the Criminal Code provisions operated effectively to catch persons who committed offences jointly or following an agreement, and that the operation of these provisions was well understood by police and lawyers, as decided cases had developed a settled understanding of the reach of these provisions.

The Criminal Code contains some provisions (sections 60A, 60B and 60C) directed to participants in ‘criminal organisations’. Such persons are prohibited from being knowingly present in a public place with two or more other persons who are also participants in a criminal organisation. Such persons may not enter or try to enter certain places as prescribed under a regulation. Such persons may not recruit or try to recruit others to become participants in a criminal organisation. At the present time, the expression ‘criminal organisation’ is effectively confined to various motorcycle gangs.7

In 2007, a non-government member of the Queensland Parliament introduced a private member’s Bill into the Legislative Assembly—the Criminal Code (Organised Criminal Groups) Amendment Bill 2007. The Bill was defeated. It proposed an offence based on participation in an organised criminal group in the following way:
A person who participated as a member of a group knowing that it was an organised criminal group, and that their participation contributed to the occurrence of any criminal activity of the group, committed a crime.

If attention is given to the notion of ‘participation’ which ‘contributes to’ activity, it seems that liability could have been proved by showing that a person had engaged in a course of conduct or contributed to a state of affairs where proof of no single fact might be sufficient to prove participation but a multiplicity of facts might.

There are other offences that depend on proof of a course of conduct. Examples include carrying on the business of unlawfully trafficking in a dangerous drug, maintaining an unlawful sexual relationship with a child, torture, and carrying on the business of providing unlawful prostitution. An example of an offence defined partly by reference to a state of affairs where no one particular fact may suffice to prove the offence is the offence of having an interest in premises used for prostitution. A person who is interested—as, say, an owner or occupier—in relation to a premises, and who knowingly allows the premises to be used for the purposes of prostitution by two or more prostitutes, commits an offence.

These offences constitute qualifications to what is known as the rule against duplicity, which is that no single charge should contain two or more separate offences. The reasons for the rule include that a court needs to know what charge it is trying in order to ensure that evidence is properly admitted and in order to ensure that a jury is properly instructed. The law is replete with examples of the difficulties that can be encountered when dealing with offences that qualify the rule against duplicity.

Formation of an opinion about the efficacy of offences directed towards those who do acts or make omissions that are designed to further the interests or objectives of a criminal group is assisted by considering what has been done in other jurisdictions which have a similar legal system to Queensland’s and which have a similar social order to this state. Obviously, the other states of Australia potentially provide a basis for comparison. However, it is to New Zealand to which regard will first be had, because of all the Australasian jurisdictions, it is the one which has had laws dealing with criminal groups in place for the lengthiest period. Provisions from some other Australian states will then be noted. Canada has also made provision for organised crime offences.

### 8.2.2 New Zealand

Problems associated with offending by gangs or groups was considered as long ago as 1987. A Committee of Inquiry into Violence made a report (Report of Ministerial Committee of Inquiry into Violence, March 1987) which, while observing that there was no simple answer to the problems associated with gangs, rejected the contention that membership of them be outlawed.

In the decade that followed, concerns grew about the extent to which some gangs were involved in organised crime. These concerns led to the drafting of the Harassment and Criminal Associations Bill 1997 (NZ). The Bill proposed a new section 98A for the Crimes Act 1961 (NZ). The provision was not designed to penalise persons solely on the basis of their association with a gang; rather, it penalised persons who knew that a gang was involved in serious offending, and who participated in the gang’s activities, intending to further the gang’s criminal conduct. The Bill became the Crimes Amendment Act (No1) 1997.

The offence applied to a person who:

- participates in any criminal gang knowing that it is a criminal gang; and
- intentionally promotes or furthers any conduct by any member of that gang that amounts to an offence or offences punishable by imprisonment.

The section defined the terms ‘member’ and ‘criminal gang’—the latter definition being linked to proof of criminal convictions of at least three gang members.

The section also included evidentiary provisions to make proof of the offence easier, for example, by allowing the prosecution to prove that the accused knew that a gang was a criminal gang by proving that a police
officer had warned the accused on at least two separate occasions that it was a criminal gang. Also, by providing that the prosecution need not prove that the accused’s conduct amounted to aiding, abetting, inciting, counselling or procuring any particular offence committed by any other person.

Having regard to later legislative developments referred to below, it is not necessary to examine the 1997 amendments. However, in an article published in 1998, *Broader Liability for Gang Accomplices: Participating in a Criminal Gang*, it was argued that section 98A was probably superfluous, because it concerned conduct already within the ambit of the party provisions (section 66) of the Crimes Act 1961 (NZ). These provisions are substantially similar to section 7–9 of the Queensland Criminal Code.

Section 98A was repealed by the Crimes Amendment Act 2002. Section 5 of that amending Act substituted a new section 98A, which was in the following terms:

**98A Participation in organised criminal group**

1. Every one is liable to imprisonment for a term not exceeding 5 years who participates (whether as a member or an associate member or prospective member) in an organised criminal group, knowing that it is an organised criminal group, and—
   a. knowing that his or her participation contributes to the occurrence of criminal activity; or
   b. reckless as to whether his or her participation may contribute to the occurrence of criminal activity.

2. For the purpose of this Act, a group is an organised criminal group if it is a group of 3 or more people who have as their objective or one of their objectives—
   a. obtaining material benefits from the commission of offences that are punishable by imprisonment for a term of 4 years or more; or
   b. obtaining material benefits from conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of offences that are punishable by imprisonment for a term of 4 years or more; or
   c. the commission of serious violent offences (within the meaning of section 312A(1)) that are punishable by imprisonment for a term of 10 years or more; or
   d. conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of serious violent offences (within the meaning of section 312A(1)) that are punishable by imprisonment for a term of 10 years or more.

3. A group of people is capable of being an organised criminal group for the purpose of this Act whether or not—
   a. some of them are subordinates or employees of others; or
   b. only some of the people involved in it at a particular time are involved in the planning, arrangement, or execution at that time of any particular action, activity, or transaction; or
   c. its membership changes from time to time.

The replacement of the previous section 98A with the new section 98A was to give effect to New Zealand’s obligations under the United Nations Convention Against Transnational Organised Crime.

Further amendments that were made in 2009 and 2012 have resulted in section 98A in the current form:

**98A Participation in organised criminal group**

1. Every person commits an offence and is liable to imprisonment for a term not exceeding 10 years who participates in an organised criminal group—
   a. knowing that 3 or more people share any 1 or more of the objectives (the particular objective or particular objectives) described in paragraphs (a) to (d) of subsection (2)
An organised crime specific offence / proceeds of crime

Queensland Organised Crime Commission of Inquiry

(whether or not the person himself or herself shares the particular objective or particular objectives); and

b. either knowing that his or her conduct contributes, or being reckless as to whether his or her conduct may contribute, to the occurrence of any criminal activity; and

c. either knowing that the criminal activity contributes, or being reckless as to whether the criminal activity may contribute, to achieving the particular objective or particular objectives of the organised criminal group.

(2) For the purposes of this Act, a group is an organised criminal group if it is a group of 3 or more people who have as their objective or one of their objectives—

a. obtaining material benefits from the commission of offences that are punishable by imprisonment for a term of 4 years or more; or

b. obtaining material benefits from conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of offences that are punishable by imprisonment for a term of 4 years or more; or

c. the commission of serious violent offences; or

d. conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of serious violent offences.

(3) A group of people is capable of being an organised criminal group for the purposes of this Act whether or not—

a. some of them are subordinates or employees of others; or

b. only some of the people involved in it at a particular time are involved in the planning, arrangement, or execution at that time of any particular action, activity, or transaction; or

c. its membership changes from time to time.

An understanding of how the provision operates can be gained from examining cases, such as those detailed below, that have considered it.

The behaviour required to be proved is ‘participation’ in an organised criminal group. The states of mind required to be proved are:

- knowledge that the group that the offender is participating in shares at least one of the particular objectives; and

- knowledge that or reckless indifference about, whether his [or her] conduct might contribute to the occurrence of any criminal activity; and

- knowledge that or reckless indifference about, whether the criminal activity contributes to achieving the particular objective of the group. 19

19.
**Case study**

**S v The Queen**

The case of *S v The Queen* concerned a charge laid under section 98A, as enacted in 2002.

S and others went to the place where their associate had been seriously assaulted, and told the mother of the suspected assailant that the ‘same thing’ would happen to the assailant and that the assailant should know that they were ‘after him’.

S was indicted on the basis that he participated in an organised criminal group, knowing that it was an organised criminal group, and for being reckless as to whether his participation might contribute to the occurrence of criminal activity, including the injuries of [the assailant], with intent to cause him grievous bodily harm.

An element to be proven in relation to the organised criminal group offence was that the group S was participating in was ‘an organised criminal group’. Under section 98A(2), a group was an organised criminal group if it was a group of three or more who had, as one of their objectives, ‘obtaining material benefits from the commission of’ a certain class of offences (section 98A(2)(a)) or the objective of ‘the commission of serious violent offences’ (section 98A(2)(c)).

The prosecution intended to prove one or both of these objectives by inference from proving the convictions of certain persons who were presently members of the group that S belonged to.

The Court ruled that it could not be safely inferred that the group had either of the objectives from the facts that some members of it had convictions. The Judge said that ‘[m]ore is required to enable the jury to draw the inference that at the time the crimes were committed, they were committed on behalf of the [group] and that they were committed as part of the objectives of the [group].’

Mr Pike QC, an officer of the Crown Law Office, Wellington, informed the Commission that the ruling made in this case was never appealed. Mr Pike said that the view was formed that as a stand-alone charge, section 98A was effectively unable to be made out. He said that the position in New Zealand now is that section 98A is relied on as an additional count in indictments charging accused persons with offences that go to prove the element in section 98A(2) of having as an objective the commission of serious violent offences.

He summed up the New Zealand position this way:

> Section 98A is seen as a useful adjunct to the application of existing law to criminal cartels but because of the difficulty of proving qualifying offending by the three or more members of a criminal cartel – and proving that the offending was for the ‘collective good’ of the gang and not freelance criminal offending, it does not have the ‘gang busting’ impact envisaged by its designers.

**8.2.3 New South Wales**

Section 93S, 93T, 93TA and 93U of the *Crimes Act 1900* (NSW) provide specific provisions dealing with criminal gangs, including an offence concerning participation in criminal groups.

Criminal gang specific provisions were first introduced into the Crimes Act in 2006, when the precursor to the current provisions (the now repealed sections 93I–93IL) were introduced by the *Crimes Legislation Amendment (Gangs) Act 2006*. The purpose of the 2006 amendments was to criminalise gang participation and gang-related activity, recognising that crimes committed by gangs ‘are a far greater threat to the safety and wellbeing of the community than most crimes committed by individuals acting alone’.

---

**An organised crime specific offence / proceeds of crime**

**Queensland Organised Crime Commission of Inquiry**

---

544 **Queensland Organised Crime Commission of Inquiry**
The amendments created a new offence of knowingly or recklessly participating in a criminal group. A further three offences were also created, applying to assaults, assaulting police, and damaging or threatening to damage property, where such conduct is committed on half of the criminal group. The provisions defined the terms ‘criminal group’ and ‘serious violent offence’, and those definitions remain unaltered in current section 93S.

The current criminal group provisions were inserted into the Crimes Act in 2012 by the Crimes Amendment (Consorting and Organised Crime) Act 2012.

Section 93S provides the relevant definitions:

The term ‘criminal group’ is defined to mean a group of three or more people who have as their objective or one of their objectives:

- obtaining material benefits from conduct that constitutes a serious indictable offence, or
- obtaining material benefits from conduct engaged in outside the State that, if it occurred in the State would be a serious indictable offence, or
- committing serious violence offences, or
- engaging in conduct outside the State that, if it occurred in the State would constitute a serious violence offence.

A ‘serious violence offence’ is one punishable by life imprisonment or at least 10 or more years’ imprisonment, where the conduct constituting the offence involves:

- loss of a person’s life or serious risk of loss of a person’s life, or
- serious injury to a person or serious risk of serious injury to a person, or
- serious damage to property in circumstances endangering the safety of any person, or
- perverting the course of justice in relation to any of the above criminal conduct.

Section 93S also provides that a group of people is capable of being a criminal group, whether or not any of them are subordinates or employees of others, or whether or not only some of those involved in the group are involved in planning, organising or carrying out any particular activity, or whether or not its membership changes from time to time.

Section 93T of the Crimes Act now provides for six offences:

The first, contained in section 93T(1), is the offence of participating in a criminal group. Section 93T(1) provides as follows:

(1) A person who participates in a criminal group is guilty of an offence if the person:

(a) knows, or ought reasonably to know, that it is a criminal group, and
(b) knows, or ought reasonably to know, that his or her participation in that group contributes to the occurrence of any criminal activity.

Maximum penalty: Imprisonment for 5 years.

A more serious offence for those who direct any of the activities of the group is provided for in section 93T(1A), which provides that:

(1A) A person who participates in a criminal group by directing any of the activities of the group is guilty of an offence if the person:

(c) knows that it is a criminal group, and
(d) knows, or is reckless as to whether, that participation contributes to the occurrence of any criminal activity.

Maximum penalty: Imprisonment for 10 years.
Sub-sections 93T(2), (3), (4) and (4A) provide as follows:

(2) A person who assaults another person, intending by that action to participate in any criminal activity of a criminal group, is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

(3) A person who destroys or damages property belonging to another person, or threatens to destroy or damage property belonging to another person, intending by that action to participate in any criminal activity of a criminal group, is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

(4) A person who assaults a law enforcement officer while in the execution of the officer’s duty intending by that action to participate in any criminal activity of a criminal group, is guilty of an offence.

Maximum penalty: Imprisonment for 14 years.

(4A) A person who participates in a criminal group whose activities are organised and on-going by directing any of the activities of the group is guilty of an offence if the person:

(e) knows that it is a criminal group, and

(f) knows, or is reckless as to whether, that participation contributes to the occurrence of any criminal activity.

Maximum penalty: Imprisonment for 15 years.

Central to the operation of section 93T is a ‘criminal group’. It is necessary to prove that the group of at least three shared a particular objective. Proving the shared objective would, in some cases, involve proof of previous acts and the drawing of inferences from the conduct proved. The difficulty of proving the objective would be, in many cases, substantial.

Section 93TA provides an offence of receiving material benefit derived from criminal activities of criminal groups.

The Commission received statistical information from the New South Wales Bureau of Crime Statistics and Research regarding finalised charges under section 93T (and former section 93IK) of the Crimes Act 1900 for the period from 2007 to June 2015. The Commission sought this information to gauge the use and impact of a specific ‘participate in a criminal group’ offence in the context of an Australian jurisdiction.

Statistics for the period 2013 to June 2015 provide an adequate ‘snapshot’, and for section 93T(1) are as follows:

- 178 charges commenced
- of the 178 charges, 94 were finalised by way of conviction (52 per cent)
- of those 94 convictions, 85 followed a plea of guilty
- of the 178 charges commenced, 77 charges were withdrawn by the prosecution (43 per cent)
- of the 178 charges, 4 were dismissed or were finalised by a not guilty finding
- of the 178 charges, 3 were transferred to the Drugs Court
- of the 94 convictions, 18 convictions represented the principal offence—that is, the offence which received the most serious penalty
- of the 18 convictions where section 93T (1) was the principal offence: 8 persons received imprisonment; 2 persons received an intensive correction order; 2 persons received a suspended sentence; 3 persons received a community service order; 3 persons received a bond.

The above statistics are informative. In a two-and-half-year period, 178 charges for section 93T(1) were commenced. Of those charges, 43 per cent were withdrawn by the prosecution and 53 per cent resulted
in a conviction. Of those convictions, only 18 convictions represented the principal offence at sentence—
that is, the offence which received the most serious penalty. Of those 18, less than half were sentenced to
actual imprisonment.

The Commission also sought information from the New South Wales Bureau of Crime Statistics and Research
to ascertain whether the offences contained in section 93T were charged as stand-alone offences or charged
in conjunction with other offence/s. On the vast majority of occasions, an offence under section 93T was
charged in conjunction with other offences. The New South Wales experience seems to accord with that
in New Zealand, where the specific offence of participating in an organised criminal group is relied on as an
additional count in indictments charging persons with ‘traditional’ criminal offences.

8.2.4 Western Australia

In 2012, the Criminal Code (WA) was amended to add sections 221C–221F.

Section 221E(1) provides an offence of participating in the activities of a criminal organisation, and section
221F(1) provides the offence of instructing the commission of an offence for the benefit of the organisation.

Section 221D(1) states that an entity is a ‘criminal organisation’ if it is a ‘declared organisation’, or if it is an
‘organisation’ whose members associate ‘for the purpose of organising, planning, facilitating, supporting or
engaging in criminal activity’, and the organisation represents a ‘risk to public safety and order in the State’.

So, unlike the position in New Zealand and New South Wales, the determination whether an organisation
is a criminal organisation will not necessarily only involve a question of fact for the court trying a person
charged with an offence against sections 221E or 221F. An entity is deemed to be a ‘criminal organisation’ if
it is declared to be so under another Act, namely, the Criminal Organisations Control Act 2012 (WA). Thus, to
the extent that a particular prosecution is against persons asserted to be members of a declared entity, the
difficulty of proving that the entity is a criminal organisation can be overcome.

Section 221E relevantly provides that:

1. A person who, for the purpose of enhancing the ability of a criminal organisation to facilitate
   an indictable offence, by an act or omission, participates in or contributes to any activity of the
   criminal organisation is guilty of a crime …

2. For the purposes of subsection (1), facilitation of an offence does not require knowledge
   of a particular offence the commission of which is facilitated, or that an offence actually
   be committed.

3. In a prosecution for an offence under subsection (1), it is not necessary to prove that –
   (a) the criminal organisation actually facilitated or committed the indictable offence; or
   (b) the participation or contribution of the accused actually enhanced the ability of the
      criminal organisation to facilitate or commit an indictable offence; or
   (c) the accused knew the specific nature of any indictable offence that may have been
      facilitated or committed by the criminal organisation; or
   (d) the accused knew the identity of any of the persons who are members of the
      criminal organisation.

Section 221F relevantly provides that:

1. A person who is a member of a criminal organisation and who instructs … any person to
   commit an offence … for the benefit of, at the direction of, or in association with, the criminal
   organisation is guilty of a crime …
(2) In a prosecution for an offence under subsection (1), it is not necessary to prove that –
   (a) an offence other than the offence under subsection (1) was actually committed; or
   (b) the accused instructed a particular person to commit an offence; or
   (c) the accused knew the identity of all the persons who are members of the criminal organisation.

8.2.5 South Australia

The *Criminal Law Consolidation Act 1935* (SA) was amended in 2012 to add sections 83D–83G.

Participating in a criminal organisation was made an offence by section 83E(1), the terms of which are very similar to section 93T(1) of the Crimes Act (NSW). The provisions of subsections 83E(2)–(4) are also very similar to subsections 93T (2)–(4) of the NSW statute.

Section 83D(1) defines a ‘criminal organisation’ as a criminal group or a declared organisation. A ‘criminal group’ is relevantly defined as a group consisting of two or more persons if either: (a) an aim or activity of the group includes engaging in conduct, or facilitating engagement in conduct, constituting a serious violence offence; or (b) an aim or activity of the group includes engaging in conduct, or facilitating engagement in conduct, constituting a serious offence that is intended to benefit the group, participants in the group, or their associates.

Like the Western Australian provision, the South Australian section allows for the possibility that a criminal organisation can be proven simply upon proof that an organisation has been declared under the provisions of another South Australian statute. Unlike the Western Australian provision—but conforming with the position in New Zealand and NSW—the South Australian provision does not require proof that the criminal organisation constitutes a risk to public safety.

8.2.6 Canada

In Canada, constitutional responsibility for criminal law rests with the federal parliament rather than with provincial legislatures, so it is only necessary to look to the Criminal Code RSC, 1985, C-46. Since 1997, the Code has contained provisions concerning offences for criminal organisations. The present provisions (sections 467.11, 467.111, 467.12 and 467.13) were amended in 2001.

Section 467.11 is in almost the same terms as that used in section 221E of the Western Australian Criminal Code. Section 467.11 relevantly provides that:

(1) Every person who, for the purpose of enhancing the ability of a criminal organization to facilitate or commit an indictable offence under this or any other Act of Parliament, knowingly, by act or omission, participates in or contributes to any activity of the criminal organization is guilty of an indictable offence ...

(2) In a prosecution for an offence under subsection (1), it is not necessary for the prosecution to prove that

   (a) the criminal organization actually facilitated or committed an indictable offence;
   (b) the participation or contribution of the accused actually enhanced the ability of the criminal organization to facilitate or commit an indictable offence;
   (c) the accused knew the specific nature of any indictable offence that may have been facilitated or committed by the criminal organization; or
(d) the accused person knew the identity of any of the persons who constitute the
criminal organization.

Section 467.13 is in substantially the same terms as section 221F of the Western Australian Code.

Section 467.1 defines a ‘criminal organization’ to mean
a group, however organized, that
(a) is composed of three or more persons in or outside Canada; and
(b) has as one of its main purposes or main activities the facilitation or commission of one or
more serious offences that if committed would likely result in the direct or indirect receipt
of a material benefit, including a financial benefit, by the group or by any persons who
constitute the group.

It does not include a group of persons that forms randomly for the immediate commission of a
single offence.

In Venneri, a decision of the Supreme Court of Canada, Fish J said that:
... by insisting that criminal groups be ‘organized’, Parliament has made plain that some form of
structure and degree of continuity are required to engage the organized crime provisions that are part
of the exceptional regime it has established under the Code. [29]

... The structured nature of targeted criminal organizations also sets them apart from criminal
conspiracies ... Stripped of the features of continuity and structure, ‘organized crime’ simply becomes
all serious crime committed by a group of three or more persons for a material benefit. Parliament
has already criminalized that activity through the offences of conspiracy, aiding and abetting, and the
‘common intention’ provisions of the Code ... [35]

### 8.3 Observations

An examination of the various ‘participation’ offences shows that a prosecuting agency would need to
prove that an accused person did an act or made an omission (participates or contributes) to further the
group’s aims or objectives with a particular state of mind. To this extent, the various provisions accord with
other criminal offences—generally those involving a course of conduct, which require proof of an act or an
omission performed with a particular state of mind.

However, in each jurisdiction, considerable complexity attends or would seem to attend the proof of an
‘organised criminal group’, ‘criminal group’ or ‘criminal organisation’. The different definitions all require that
it be proved that the alleged groups have, as an objective or aim, the commission of offences, generally of
a stated level of seriousness, and, in the case of some, for the purpose of gaining material benefits. Proving
that at least two—or in most cases three—people share the same objective is extraordinarily difficult, if for
no other reason than that the evidence relied upon must be admissible against the one (or more than one)
person charged, who may or may not be one of the two or three whose conduct is relied upon to prove the
existence of the group or organisation.

These offences require proof that there is a structure of some form or coordination of some form in order to
show the existence of a group or association or organisation. A definition of a group or organisation arguably
requires a ‘flexible definition that is capable of capturing criminal organisations in all their protean forms’,22 but
not a definition so flexible that it captures a group who band together to put graffiti on public property from
time to time. Definitions that require proof of obtaining material benefits undoubtedly go much of the way
towards excluding the band last mentioned, but those definitions, in seeking to avoid capturing some groups,
introduce a further element required to be proven.
In the final report of the Australian Royal Commission of Inquiry into Drugs,23 the Honourable Justice ES Williams said that definitions of a phrase like ‘organised crime’ arguably ‘detract attention from the task of effectively dealing with criminal activity.’ He went on to say that the characteristics of those engaged in criminal activity on an organised basis were not confined to formalised structures with predefined powers, responsibilities and functions.

The definitional difficulty identified by Sir Edward Williams in 1980 would seem to still bedevil this area of legislative activity and of policing. For example, the Commission asked Deputy Commissioner Barnett of the QPS to provide it with the names and addresses of any persons, businesses or organisations that, since 1 January 2013, have complained to the QPS to have been affected by criminal activity, which the QPS then regarded or even now regards as organised criminal activity. In answering the notice,24 Deputy Commissioner Barnett said that the QPS does not, beyond complaints about outlaw motorcycle gangs, record complaints within an organised crime context. To comply with the Commission’s request would have required members of the QPS to identify every offence reported, and to review each one to determine whether the offence reported was related to organised crime. Deputy Commissioner Barnett attributed the difficulty to the absence of a consistent definition of organised crime against which to assess whether a particular report fell within the understanding of organised crime.

One of the purposes of the Police Powers and Responsibilities Act 2000 (Qld) is to provide powers to police that are necessary for effective modern policing and law enforcement. The phrase ‘organised crime’ is defined in that Act to mean ‘an on-going criminal enterprise to commit serious indictable offences in a systematic way involving a number of people and substantial planning and organisation’.

The Commission asked Deputy Commissioner Barnett whether the QPS considered that this definition afforded adequate guidance to it in assessing whether an incident or incidents fell within the category of organised crime. In answering the notice,25 Deputy Commissioner Barnett said that notions of organised crime had progressed beyond highly structured, long standing, organised syndicates, as criminals now often entered into short-term arrangements. This makes it difficult for the police to demonstrate substantial planning for the purposes of obtaining covert warrants, which are needed to enter premises for the purposes of investigating organised crime. He said that, in the time since 1 January 2013, only two applications had been made to the Supreme Court for covert warrants to enter and search for evidence of organised crime. The Deputy Commissioner said that networks for distributing material such as dangerous drugs, child exploitation images and personal identification information had become ‘more disconnected, rather than organised, as a result of opportunities provided by the dark web’.

The former Director of Public Prosecutions, Mr AW Moynihan QC, advised the Commission that the ODPP does not keep any records that distinguish between ‘organised crime offending and other types of criminal conduct’.

The Commission invited the Bar Association of Queensland and the Queensland Law Society to put forward any view that those bodies had regarding the need for an offence to be added to the Criminal Code dealing with organised criminal activity. The Queensland Law Society did not support the enactment of such an offence, contending that the regime currently provided for by the Criminal Code was adequate. The Bar Association of Queensland did not advocate a view either way, but did point out that defining organised crime for the purposes of an offence required care to ensure that any definition was not so broad as to encompass groups or associations engaged in minor criminal activity.

It is the Commission’s view that, having regard to the legislative examples from other jurisdictions, the enactment of an organised crime offence will more likely than not result in an offence that will be much more difficult to prove than the wide range of offences currently available in the Criminal Code. Accordingly, the Commission queries the utility of enacting such an offence.

Reliance upon the party provisions of the Criminal Code (sections 7, 8 and 9), the terms of which are well-understood by those practising in the field of criminal law, mean that the police and prosecution are well-placed to prove cases against those engaged in organised criminal activity.
The offence of trafficking provides an example. Section 5 of the Drugs Misuse Act provides that any person who carries on the business of unlawfully trafficking in a dangerous drug commits a crime. This crime is generally established upon proof of the sale, usually repeatedly, of drugs. However, all the activities that are usually associated with the sourcing, purchasing, storing, marketing and selling of products and recovering monies owed from sales are forms of conduct arguably relevant to proof that a person has engaged in the business of unlawfully trafficking in a dangerous drug.

By virtue of section 7 of the Criminal Code, it is not necessary to prove a case of trafficking to show that a person was engaged in all of these activities. A person who aids another to recover monies owed—provided it is established that he or she knew that he or she was assisting to recover funds owed from drug sales—would be susceptible to being found guilty of trafficking, irrespective of any benefits he or she received in return. A person who procured another to run the business on his or her behalf would also be susceptible to being found guilty of trafficking.

Upon a conviction for trafficking, a sentencing court must have regard to a wide variety of factors in sentencing. The Penalties and Sentences Act 1992 (Qld), section 9, requires a court to have regard to factors such as the nature and seriousness of the offending. So the level of sentences imposed on the various offenders in a trafficking operation will reflect the roles played in the operation, the level of profit achieved, and the degree of sophistication of the operation. Offenders who organise or direct the trafficking normally receive the sternest sentences.

The information provided by Deputy Commissioner Barnett and referred to above suggests to the Commission that the QPS has not found the descriptor ‘organised crime’ to be a useful one in the discharge of its statutory responsibility to detect offenders and bring them to justice.26

8.4 Proceeds of crime

The main object of the Criminal Proceeds Confiscation Act 2002 (Qld) is to remove the financial gain and increase the financial loss associated with illegal activity—irrespective of whether a particular person is convicted of an offence because of the activity.27 Other important objects include depriving persons of illegally acquired property and benefits derived from the commission of offences, depriving persons of wealth that those persons cannot show was lawfully acquired, assisting law enforcement agencies to effectively trace property acquired by persons who engage in illegal activity and benefits derived from the commission of offences, and forfeiting to the State the property of persons who commit certain offences.

To achieve these and other objectives, the Act provides for three separate schemes. Chapter 2 of the Act is administered by the Crime and Corruption Commission and allows for the confiscation of assets, whether or not a person has been convicted of any offence or even charged. Chapter 2 includes the ‘unexplained wealth’ provisions that enable the Court to order the confiscation of a person’s assets, unless the person can prove those assets were lawfully acquired.

The Crime and Corruption Commission (CCC) also administers chapter 2A of the Criminal Proceeds Confiscation Act, which is the serious drug offender confiscation order scheme. This scheme concerns the conviction of particular serious offences involving drugs, and allows the State to apply to have all of the convicted person’s property forfeited to the State. Upon application, the Court must make such an order if satisfied the respondent has been convicted of a relevant offence for which the required certificate has been issued, and that the application was made within six months after the issuing of the certificate. The Court may refuse to make the serious drug offender confiscation order if satisfied that it is not in the public interest to make the order.

The third scheme is administered by the Director of Public Prosecutions, and is provided for in chapter 3 of the Act. The scheme depends upon a person being charged and convicted of a ‘confiscation offence’, which includes an indictable offence punishable by at least 5 years imprisonment.
Court proceedings under chapters 2 and 2A are conducted by officers of the ODPP, who act on instructions provided by the CCC. This situation comes about by virtue of a provision of the Act, notwithstanding that the Act provides that the chapters 2 and 2A schemes are to be administered by the CCC. Court proceedings under chapter 3 are also conducted by officers of ODPP; however, in those proceedings, the officers act on the instructions of the Confiscations Unit in the ODPP.

In submissions made to this Commission, both the former Director of Public Prosecutions, Mr AW Moynihan QC, and the CCC contend that greater efficiencies could be achieved if the CCC administered all three schemes, and if it conducted court proceedings in relation to the schemes. The CCC pointed to the consideration that it has staff trained in police and financial investigations. The former Director of Public Prosecutions acknowledged that this consideration has validity. Additionally, the Director made the point that when the Act commenced, the division of responsibility was based on whether the scheme concerned was conviction-based or not. However, when chapter 2A was inserted, a conviction-based scheme was then administered by the CCC, and so there is now no longer any compelling reason why that entity, if agreeable to administering the chapter 3 scheme, should not do so.

The Commission notes the 2013 Report of the Independent Advisory Panel – Review of the Crime and Misconduct Act and Related Matters. The report was the culmination of the independent review carried out by the Honourable Ian Callinan and Professor Nicholas Aroney. Recommendation 7 of the report is that, save for urgent applications in pending matters, the powers of the Director of Public Prosecutions for the criminal proceeds confiscation regime (under the Criminal Proceeds Confiscation Act) ought to be vested in the CCC. The recommendation came with the caveat that the CCC satisfy the Executive Government that it has the legal and accounting capacity extending to a knowledge of accounts, financial affairs, commercial law, property law, trusts, equity and tracing to administer the convictions-based scheme.

In its submission to the Commission, the CCC assured the Commission of its police investigating skills, financial investigation skills, legal skills and property administration skills.

### Recommendation

8.1 The Commission recommends that the Queensland Government amend the Criminal Proceeds Confiscation Act 2002, so that the Crime and Corruption Commission administer the Chapter 3 scheme, and the Crime and Corruption Commission conduct all court proceedings under the Act.

### (Endnotes)

1. Commission of Inquiry Order (No 1) 2015, paras 3(g), 10(h).
2. Section 137 Criminal Organisation Act 2009 (Qld) provides that the Act will expire seven years after commencement.
3. Section 130 Criminal Organisation Act 2009 (Qld) provides that the Act must be reviewed after five years after commencement.
6. Section 9 Criminal Code 1899 (Qld).
7. The Commission is unaware of the other limbs of the definition of ‘criminal organisation’ contained in Section 4 of the Criminal Code 1899 (Qld), having been relied on.
8. Section 5 Drugs Misuse Act 1986 (Qld).
9. Section 229B Criminal Code 1899 (Qld).
10. Section 320A Criminal Code 1899 (Qld).
<table>
<thead>
<tr>
<th>No.</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Section 229HB Criminal Code 1899 (Qld).</td>
</tr>
<tr>
<td>12</td>
<td>Section 229K Criminal Code 1899 (Qld).</td>
</tr>
<tr>
<td>13</td>
<td>S v The Queen (1989) 168 CLR 266 at 284; Section 567 Criminal Code 1899 (Qld).</td>
</tr>
<tr>
<td>14</td>
<td>Explanatory Notes to the Harassment and Criminal Associations Bill 1997 (NZ), p. i.</td>
</tr>
<tr>
<td>16</td>
<td>That is, conduct that would fall within the Parties to offences section of the Crimes Act 1961 (NZ).</td>
</tr>
<tr>
<td>18</td>
<td>R v Mitford [2005] 1 NZLR 753 at 38.</td>
</tr>
<tr>
<td>20</td>
<td>High Court, Paterson J, 13 May 2004.</td>
</tr>
<tr>
<td>21</td>
<td>Explanatory Notes to the Crimes Legislation Amendment (Gangs) Bill 2006.</td>
</tr>
<tr>
<td>22</td>
<td>R v Terezakis (2007) 223 CCC (3d) 344 at 34.</td>
</tr>
<tr>
<td>26</td>
<td>Section 2.3(d) Police Service Administration Act 1990.</td>
</tr>
<tr>
<td>27</td>
<td>Section 4 Criminal Proceeds Confiscation Act 2002 (Qld).</td>
</tr>
</tbody>
</table>
Appendix 1

Terms of Reference

Commissions of Inquiry Order (No. 1) 2015

Short title

1. This Order in Council may be cited as the Commissions of Inquiry Order (No. 1) 2015.

Commencement

2. This Order in Council commences on 1 of May 2015.

Appointment of Commission

3. UNDER the provisions of the Commissions of Inquiry Act 1950 the Governor in Council hereby appoints Michael Byrne QC, from 1 of May 2015, to make full and careful inquiry in an open and independent manner with respect to the following matters:

   a. the extent and nature, and economic and societal impacts (including impacts on individuals) of organised crime in Queensland with particular emphasis on the key areas of focus;

   b. the key areas of focus are:

      • the high threat illicit drug and/or precursor markets, including but not limited to methylamphetamine, cocaine, heroin, drug analogues and new psychoactive substances, 3, 4 - Methyleneoxymethamphetamine and cannabis;

      • internet or electronic or technology enabled child sexual offending, including the child exploitation material market;

      • financial crimes – primarily investment and financial market fraud and financial data theft; and

      • the relationship between organised crime and corruption in Queensland.

   c. the extent to which entities involved in organised crime, use, or provide the services of, activities that enable or facilitate organised crime in Queensland with particular emphasis on the key enablers;
d. the key enablers are:
   • money laundering;
   • cyber and technology-enabled crime;
   • identity crime;
   • violence and extortion; and
   • professional facilitators, including but not limited to accountants, lawyers, financial advisers, real estate agents, IT experts, technical security experts and chemists.

e. the adequacy and appropriateness of the current responses of Queensland law enforcement, Queensland intelligence and Queensland prosecution agencies to prevent and combat organised crime in Queensland, including through the recovery of proceeds of crime;

f. the adequacy of current cross-jurisdictional arrangements, including the effective cooperation of Queensland law enforcement agencies with Commonwealth law enforcement agencies;

g. the adequacy of current legislation and resources available to law enforcement, criminal intelligence and prosecution agencies in Queensland to prevent and effectively investigate and prosecute organised criminal activity, including the recovery of proceeds of crime; and

h. likely future trends in organised crime, including involvement in emerging illicit and legitimate markets.

4. AND the Commission will carry out its inquiry by calling on law enforcement, intelligence and prosecution agencies, academics and relevant industry; and reviewing relevant literature and data.

5. FURTHER, in carrying out the inquiry the Commission can have regard to the experiences of individuals and other entities directly or indirectly affected by organised crime to the extent the Commission considers relevant.

6. AND in receiving evidence or information pursuant to clauses 4 and 5 on a matter that is the subject of a covert investigation or may expose a witness to risk of harm, the Commission will receive such evidence in camera and ensure anonymity of the relevant parties.

7. AND the Commission will ensure that it does not publicly expose details of current or anticipated intelligence collection strategies and investigation methods where such detail is not already in the public domain.

8. EXCEPT that the Commission is not to have regard to any matter that is currently the subject of a judicial proceeding, or a proceeding before an administrative tribunal or a commission (including but not limited to, a tribunal or commission established under a law of the Commonwealth).

Commission to report

9. AND directs that the Commissioner make full and faithful report and recommendations which he considers appropriate on the aforesaid subject matter of inquiry, and transmit the same to the Honourable the Premier by 30 October 2015.

10. WITHOUT limiting the scope of any report arising out of the inquiry, the report should:
   a. identify current and emerging organised crime threats and identify the high risk threats;
   b. outline the nature and extent of the involvement of organised crime threats, in particular high risk organised crime threats, in the key areas of focus, key enabling activities and other illicit markets;
   c. identify the illicit markets that pose a risk of harm to the Queensland community and identify those markets that pose the greatest risk of harm;
   d. identify vulnerabilities in existing systems that may facilitate organised crime;
e. highlight the current gaps within the knowledge of Queensland law enforcement agencies of the crime environment and suggest priority areas for intelligence collection;

f. evaluate the responses of law enforcement, intelligence and prosecution agencies to combating organised crime including cross-jurisdictional arrangements;

g. evaluate proactive strategies of law enforcement and intelligence agencies to maximise the reduction of risk to the community of Queensland and to prevent, disable or disrupt activities of organised crime; and

h. evaluate the adequacy of legislation and resources available to law enforcement and intelligence and prosecution agencies to effectively address organised criminal activity.

Commission to make recommendations

11. WITHOUT limiting the scope of any recommendations arising out of the inquiry, the recommendations should identify current and emerging organised crime threats, identifying those high risk threats, particularising the areas of focus which should have the highest priorities for the government and law enforcement.

Application of Act

12. THE provisions of the Commissions of Inquiry Act 1950 shall be applicable for the purposes of this inquiry including that the Commissioner may hold public or private hearings in such a manner and in such locations as may be necessary and convenient.

Endnotes

1 Made by the Governor in Council on 26 March 2015.

2 Notified in the Gazette on 2 April 2015.

3 Not required to be laid before the Legislative Assembly.

4 The administering agency is the Department of Justice and Attorney-General.
Appendix 2

Establishment and operations

The Commission reported on time and well under the budget approved by the Cabinet Budget Review Committee.

Pre-commencement

The Commissioner’s appointment and statutory powers commenced on 1 May 2015.

The Executive Director commenced on 7 April 2015 and during that month finalised the establishment of the Commission’s premises, recruited non-legal staff, began the recruitment process for legal staff, consulted on the development of the Commission’s website and made other operational arrangements.

Throughout April, background literature research was carried out, focusing on the key areas as outlined in the Terms of Reference, and to this end the Commission particularly thanks the support of the Crown Law Library.

Necessary procedural guidelines were drafted and settled by the Commissioner.

On 24 April 2015, a call for information was posted on the Commission’s website. Public notices appeared in *The Courier-Mail* and *The Australian* on 29 April and 2 May 2015 in which a call for information, contact details and information on the Terms of Reference were outlined.

The Commission officially commenced operations on 1 May 2015 in the State Law Building (50 Ann Street, Brisbane).

Evidence collection

The Commission conducted its Inquiry under the *Commissions of Inquiry Act 1950*.

Paragraph 4 of the Terms of Reference required the Commission to gather information by calling on law enforcement, intelligence, and prosecution agencies, as well as academics and relevant industry, and by reviewing relevant literature and data. Paragraph 5 of the Terms of Reference allowed the Commission to have regard to the experiences of individuals and other entities directly or indirectly affected by organised crime.

The Commission obtained information and evidence by a range of methods. As outlined, the Commission called for information. In the first weeks of commencement, the Commission met with the following key stakeholders, inviting submissions from those agencies on the Terms of Reference:

- Queensland Police Service
- Crime and Corruption Commission
- Director of Public Prosecutions
- Legal Aid Queensland
- Queensland Law Society
- Bar Association of Queensland
- Legal Services Commission Queensland
- Integrity Commissioner, Australian Commission for Law Enforcement Integrity.

The Commission also wrote to the following entities, alerting them to the Inquiry and inviting a submission:

- Queensland University of Technology
- University of Queensland
- Griffith University
- Bond University
• James Cook University
• University of Southern Queensland
• Pharmacy Board of Australia
• Association of Financial Advisors
• Australian Information Industry Association
• IT Queensland
• Australian Competition and Consumer Commission
• Institute of Public Accountants
• CPA Australia
• Chartered Accountants of Australia and New Zealand
• Real Estate Institute of Queensland
• Australian Crime Commission
• Australian Federal Police
• Together Queensland
• Queensland Police Union of Employees
• Queensland Council of Civil Liberties
• Queensland Police Commissioned Officers’ Union of Employees
• Dr Caitlin Byrne (Bond University)
• Mr Terry Goldsworthy (Bond University)
• Gold Coast Central Chamber of Commerce
• Mr Ken Gamble (private investigator).

The nature and subject matter of the Inquiry did not readily lend itself to public hearings. The majority of the submissions and information provided to the Commission were done so with reasonable requests for confidentiality.

The Commission relied on its powers under the Commissions of Inquiry Act 1950 to seek information and documents from organisations and individuals with particular knowledge. A number of individuals were interviewed and in camera hearings were held.

Due to the scope of the Commission’s Terms of Reference and the six-month timeframe for reporting it was decided that the Commission would not investigate specific complaints of criminal activity. However, the Commission received numerous complaints regarding fraudulent investment schemes. The Commission established a formal arrangement with the Queensland Police Service through a Memorandum of Understanding to refer complaints of investment or finance market fraud to the Queensland Police Service to be assessed and investigated if the complaint involves possible criminal offending.

**Hearings**

Hearings were conducted in courtroom 17, level 4 of the Brisbane Magistrates Court at 363 George Street, Brisbane. The Commission thanks the Department of Justice and Attorney-General and Chief Magistrate Judge Rinaudo.

The Commission held six days of in-camera hearings during which nine witnesses appeared. It was determined that due to the nature and subject of the material to be examined during the hearings that they would be closed to the public.

**Staffing**

Commission staff commenced progressively during April and May 2015. The Commission engaged 21 full-time equivalent staff, which comprised 11 legal staff (including the Commissioner and three counsel assisting) and 10 non-legal staff. The staff and their positions are listed in Appendix 4.
Staff came from a variety of backgrounds which resulted in a diverse range of skills and expertise. Staff were subject to criminal history checks undertaken by the Queensland Police Service, and were required to disclose any possible conflict of interest.

As the report reached its final stages, staff numbers were progressively reduced.

Statistics

The following statistics provide an overview of the Commission’s work:

- 75 submissions were received
- 105 requests for written information were issued
- 43 requests for the provision of documents were issued
- nine summonses for attendance at a hearing were issued
- six in camera hearing days were held
- 25 requests for attendance to be interviewed were issued.

In addition to requests for attendance to be interviewed, the Commission held a number of voluntary interviews with persons with relevant information.

External Engagements

The Commission engaged a number of external contractors. Below is a list of contractors and their purpose:

- Auscript – recording and transcription services
- Law in Order – dataroom services and transcription services
- Mariart – design and layout services for the Commission’s Report
- Kimberly Ellis, Editor – editorial services
- Donna Rumpf, Court Reporter – transcription services
- Helen Lubke, Court Reporter – transcription services
- Greg Henderson, Photographer – photography services

Records Management

The Commission used the records management system of the Department of Justice and Attorney-General (eDOCS) to manage its records throughout the life of the Commission.

The Commission’s records have been managed in accordance with the Commission of Inquiry Retention and Disposal Schedule (QDAN 676 v2) issued by the Queensland State Archivist (QSA) under the Public Records Act 2002. At the completion of the Commission its records (excluding administrative documents) were accepted by QSA with temporary administrative records transitioned to the Department of Justice and Attorney-General as custodian. The Commission undertook the process of applying Restricted Access Periods to both temporary and permanent records. The Department of Justice and Attorney-General is the custodian of the electronic records of the Commission.

Applications to access the Commission’s records should be made to the Department of Justice and Attorney-General by writing to GPO Box 149, Brisbane Qld 4001 or mailbox@justice.qld.gov.au.
Appendix 3

Parties granted authority to appear

<table>
<thead>
<tr>
<th>Party</th>
<th>Represented by</th>
<th>Instructed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>The State of Queensland</td>
<td>Mr Shane Doyle QC</td>
<td>Crown Law</td>
</tr>
<tr>
<td></td>
<td>Mr Benjamin MacMillan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mr Thomas Pincus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mr Matthew Hickey</td>
<td></td>
</tr>
<tr>
<td>Crime and Corruption Commission</td>
<td>Mr Anthony Glynn QC</td>
<td>Crime and Corruption Commission</td>
</tr>
<tr>
<td>Legal Aid Queensland</td>
<td>Mr John Allen QC</td>
<td>Legal Aid Queensland</td>
</tr>
</tbody>
</table>

*The Australian Crime Commission was granted leave to make submissions at the in-camera hearing on 26 June 2015. Mr David Kent QC appeared and was instructed by the Australian Government Solicitor.*
Appendices

Appendix 4

Commission staff

Commissioner
Mr Michael Byrne QC

Counsel Assisting
Mr Michael Copley QC
Ms Julie Sharp
Ms Penny White

Executive Director
Ms Louise Shephard

Principal Legal Officers
Mr Nick Hanly
Ms Jessica Horne
Ms Clare Kelly

Legal Officers
Ms Lauren Archer
Mr Michael Shears
Ms Anna Woodall
Ms Maria Zappala

Paralegals
Mr Tom Clayworth
Mr Daniel Popple

Police Officer
Detective Inspector Peter Brewer

Executive Officer
Mr Alex Robynson

Media Officer
Ms Elizabeth Edmiston

Office Manager
Ms Justine Hodgman

Records Officer
Ms Jessica Eggleton

Administration Officers
Ms Susy McKeen
Ms Azalia Torres
Appendix 5

Statistics provided by the New South Wales Bureau of Crime Statistics and Research
Number of finalised charges under sections 93T and 93JK of the Crimes Act 1900 by outcome and jurisdiction

<table>
<thead>
<tr>
<th>Section</th>
<th>Description and Lawpart</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>93T(1)</td>
<td>Participate criminal group contribute criminal activity-T2 - Lawpart 76994</td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentence committal</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Withdrawn by prosecution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transferred to the Drug Court</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Taken into account on Form 1</td>
</tr>
<tr>
<td>93T(2)</td>
<td>Participate in criminal group assist criminal activity-T2 - Lawpart 62914</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty verdict</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty verdict by jury</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Withdrawn by prosecution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deceased</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Taken into account on Form 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plea to other charge accepted in full discharge of indictment</td>
</tr>
<tr>
<td>93T(3)</td>
<td>Knowingly participate in criminal group assist crime-T1 - Lawpart 76995</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty verdict</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentence committal</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Taken into account on Form 1</td>
</tr>
<tr>
<td>93T(4)</td>
<td>Assault person intend criminal activity of criminal group-T1 - Lawpart 62915</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Withdrawn by prosecution</td>
</tr>
<tr>
<td>93T(5)</td>
<td>Destroy/damage property intend criminal activity of group-T1 - Lawpart 76996</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Withdrawn by prosecution</td>
</tr>
<tr>
<td>93T(6)</td>
<td>Knowingly direct activities of criminal group-T1 - Lawpart 76997</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Taken into account on Form 1</td>
</tr>
<tr>
<td>93JK(1)</td>
<td>Participate in criminal group assist criminal activity-T2 - Lawpart 60717</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
<tr>
<td></td>
<td>Not guilty finding</td>
<td>Not guilty finding/dismissed</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Remitted to Local/Children’s Court</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Taken into account on Form 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plea to other charge accepted in full discharge of indictment</td>
</tr>
<tr>
<td>93JK(2)</td>
<td>Assault person intend criminal activity of criminal group-T1 - Lawpart 60718</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Withdrawn by prosecution</td>
</tr>
<tr>
<td>93JK(3)</td>
<td>Destroy/damage property intend criminal activity of group-T1 - Lawpart 60719</td>
<td>Guilty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guilty plea after committal for trial</td>
</tr>
</tbody>
</table>

Note: These figures are the number of charges brought, rather than the number of persons charged. A charge refers to an instance of a particular type of offence being charged against a person.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Children's Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>District Court</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Notes:
Lawpart 96994 commenced on 09/04/2012
Lawpart 62914 commenced on 27/08/2007 and was valid to 08/04/2012
Lawpart 76995 commenced on 09/04/2012
Lawpart 62915 commenced on 27/09/2007
Lawpart 62916 commenced on 27/09/2007
Lawpart 76996 commenced on 09/04/2012
Lawpart 60717 commenced on 15/12/2006 and was valid to 26/09/2007
Lawpart 60718 commenced on 15/12/2006 and was valid to 26/09/2007
Lawpart 60719 commenced on 15/12/2006 and was valid to 26/09/2007
There were no charges finalised under section 931(1), (2) or (3) between 15/12/2006 and 31/12/2006
### NSW Criminal Court Statistics 2007 to June 2015

Number of persons found guilty whose principal offence* was under sections 93T and 93IK of the Crimes Act 1900 by penalty and jurisdiction

<table>
<thead>
<tr>
<th>Section</th>
<th>Description and Lawpart</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>93T(1)</td>
<td>Participate criminal group contribute criminal activity-T2 - Lawpart 76994</td>
<td>Imprisonment, Intensive correction order, Suspended sentence without supervision, Community Service Order, Bond without supervision, Bond without conviction, Total</td>
</tr>
<tr>
<td>93T(1A)</td>
<td>Knowingly participate in criminal group assist crime-T1 - Lawpart 76995</td>
<td>Imprisonment, Suspended sentence without supervision, Community Service Order, Total</td>
</tr>
<tr>
<td>93T(3)</td>
<td>Destroy/damage property intend criminal activity of group-T1 - Lawpart 62916</td>
<td>Imprisonment, Total</td>
</tr>
<tr>
<td>93T(4A)</td>
<td>Knowingly direct activities of criminal group-T1 - Lawpart 62915</td>
<td>Imprisonment, Total</td>
</tr>
<tr>
<td>93IK(1)</td>
<td>Participate in criminal group assist criminal activity-T2 - Lawpart 62914</td>
<td>Imprisonment, Home detention, Suspended sentence with supervision, Community Service Order, Bond with supervision, Bond without supervision, Total</td>
</tr>
<tr>
<td>93IK(3)</td>
<td>Destroy/damage property intend criminal activity of group-T1 - Lawpart 60719</td>
<td>Suspended sentence with supervision, Total</td>
</tr>
</tbody>
</table>

**Source:** NSW Bureau of Crime Statistics and Research: sr15-13324, 2015.

*Where a person has been found guilty of more than one offence, the offence which received the most serious penalty is the principal offence.

**Notes:**
- Lawpart 96994 commenced on 09/04/2012
- Lawpart 62914 commenced on 27/08/2007 and was valid to 08/04/2012
- Lawpart 76995 commenced on 09/04/2012
- Lawpart 62915 commenced on 27/09/2007
- Lawpart 62916 commenced on 09/04/2012
- Lawpart 62917 commenced on 15/12/2006 and was valid to 26/09/2007
- Lawpart 60717 commenced on 15/12/2006 and was valid to 26/09/2007
- Lawpart 60718 commenced on 15/12/2006 and was valid to 26/09/2007
- Lawpart 60719 commenced on 15/12/2006 and was valid to 26/09/2007

There were no persons found guilty under any of the relevant sections between 15/12/2006 and 31/12/2007
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>93T(1)</strong></td>
<td>2 3 2 7</td>
<td>2 2</td>
<td>2 2</td>
<td>0 1 2 3</td>
<td>0 1 1 0 1 3 4</td>
<td>0 1 1 2 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93T(1A)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(1)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td><strong>93IK(3)</strong></td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>

**Notes:**
- Lawpart 96994 commenced on 09/04/2012
- Lawpart 62914 commenced on 27/08/2007 and was valid to 08/04/2012
- Lawpart 76995 commenced on 09/04/2012
- Lawpart 62915 commenced on 27/09/2007
- Lawpart 62916 commenced on 27/09/2007
- Lawpart 76996 commenced on 09/04/2012
- Lawpart 60717 commenced on 15/12/2006 and was valid to 26/09/2007
- Lawpart 60718 commenced on 15/12/2006 and was valid to 26/09/2007
- Lawpart 60719 commenced on 15/12/2006 and was valid to 26/09/2007
- There were no persons found guilty under any of the relevant sections between 15/12/2006 and 31/12/2007.
### NSW Criminal Courts Statistics January 2007 to June 2015

Number of people charged with offences under sections 93T(1), 93T(1A), 93T(2), 93T(3), 93T(4A), 93TA(1), 93IK(1), 93IK(2) and 93IK(3) of the Crimes Act 1900

by jurisdiction, whether these were used as a stand-alone charge OR used in conjunction with other offence(s) and year.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Supreme Courts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Used as a stand-alone</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Used in conjunction</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>District Courts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>164</td>
<td></td>
</tr>
<tr>
<td>Used as a stand-alone</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Used in conjunction</td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>24</td>
<td>19</td>
<td>25</td>
<td>38</td>
<td>29</td>
<td>18</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>25</td>
<td>21</td>
<td>25</td>
<td>38</td>
<td>31</td>
<td>18</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Courts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>338</td>
<td></td>
</tr>
<tr>
<td>Used as a stand-alone</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Used in conjunction</td>
<td>7</td>
<td>34</td>
<td>22</td>
<td>46</td>
<td>47</td>
<td>66</td>
<td>42</td>
<td>35</td>
<td>39</td>
<td>153</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>8</td>
<td>41</td>
<td>27</td>
<td>49</td>
<td>54</td>
<td>73</td>
<td>48</td>
<td>41</td>
<td>47</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children’s Courts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>Used as a stand-alone</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Used in conjunction</td>
<td>7</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>2</td>
<td>1</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>9</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>2</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>7</td>
<td>5</td>
<td>4</td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>8</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>50</td>
<td>32</td>
<td>76</td>
<td>78</td>
<td>100</td>
<td>91</td>
<td>66</td>
<td>58</td>
<td>565</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>57</td>
<td>37</td>
<td>80</td>
<td>87</td>
<td>107</td>
<td>97</td>
<td>74</td>
<td>66</td>
<td>622</td>
</tr>
</tbody>
</table>
