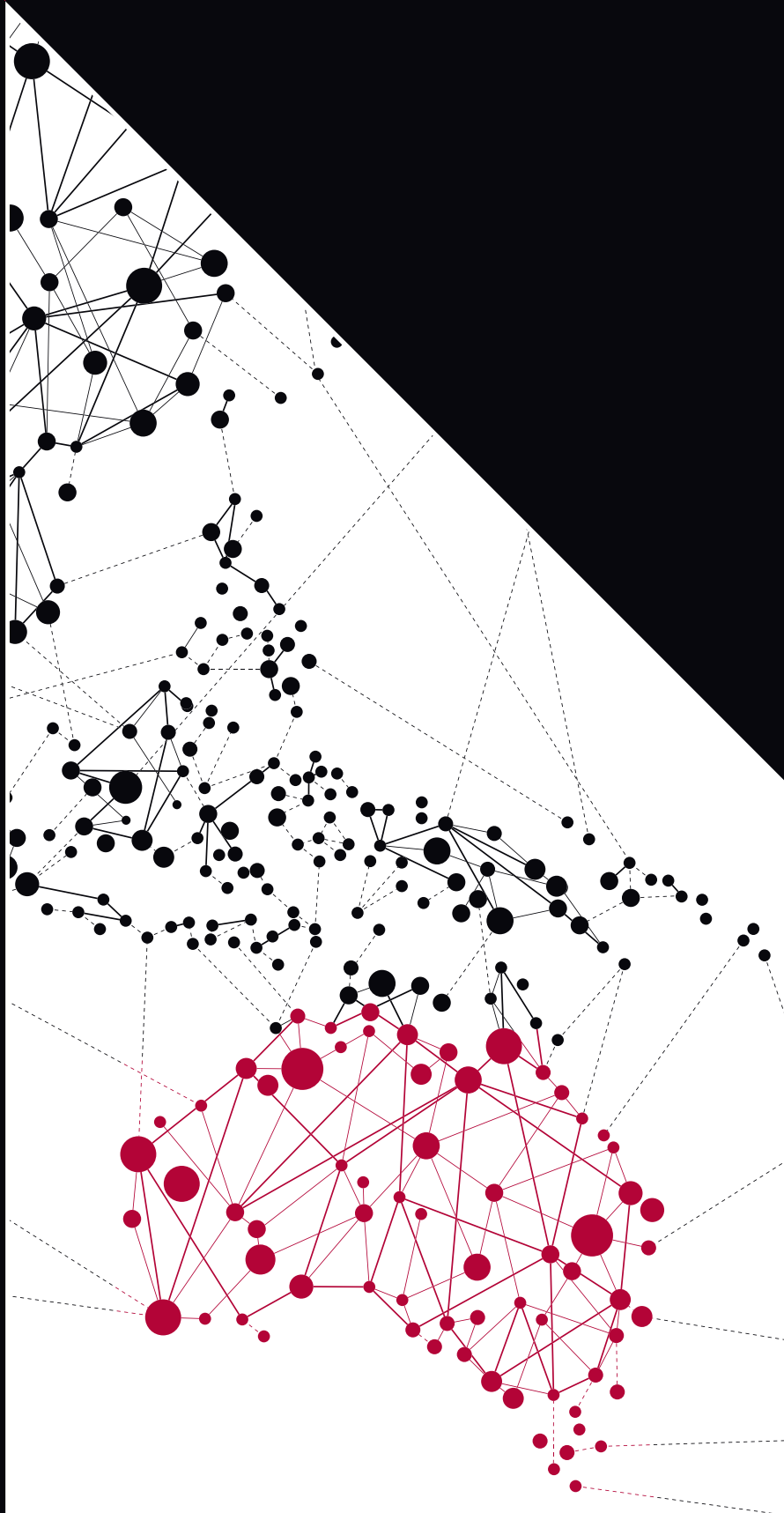




Organised Crime in Australia 2015



Correspondence should be addressed to:

Chief Executive Officer
Australian Crime Commission
PO Box 1936 Canberra City
ACT 2601

Telephone:

02 6243 6666 (from within Australia)
61 2 6243 6666 (international)

Facsimile:

02 6243 6687 (from within Australia)
61 2 6243 6687 (international)

Published May 2015

© Commonwealth of Australia 2015.

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without written permission from the Chief Executive Officer, Australian Crime Commission.

ISSN 2202-3925



CEO FOREWORD

MR CHRIS DAWSON APM



Organised Crime in Australia 2015 is the Australian Crime Commission's biennial public report that delivers a current picture of the serious and organised crime environment in Australia. It outlines the existing and emerging organised crime threats impacting the Australian community and national interests.

Serious and organised crime is growing in sophistication and constantly adopting new and advanced technologies to undertake illegal activities. It exploits the internet and other technologies to target the community through activities such as online scams, cybercrime and the theft of personal identity information stored electronically. It is expanding its reach globally and injecting itself into new markets—both legitimate and illegitimate—in order to increase its opportunities to generate illicit wealth. It works to conceal unlawfully derived profits, seeking to intermingle those funds with legitimately earned money.

These activities significantly affect the wellbeing of families and communities across Australia. Serious and organised crime diverts funds out of the legitimate economy and undermines the profitability of lawful businesses. It removes large amounts of money from the Australian economy that could otherwise be used to fund services, roads, hospitals and schools. This money is instead lining the pockets of criminals.

The presence of organised crime and its impact on the community is pervasive and law enforcement and partners are working together to ensure our activities are well coordinated and cohesive.


The Australian Crime Commission's work is critical in determining how Australia responds to the threat of serious and organised crime. We work across borders to discover, understand and respond to the highest risk serious and organised crime threats.

- We proactively **discover** new and emerging threats and fill the gaps in our intelligence.
- We maintain a national intelligence picture on current and emerging threats, supported by our partners, to **understand** the organised crime environment and its impact on the community. We use this intelligence to inform our responses to serious and organised crime.
- We **respond** to the serious and organised crime threat by disrupting, disabling and dismantling criminal enterprises through effective enforcement, regulation, policy and legislation.

Our priority is to reduce the impact of serious and organised crime on the community, by making it harder for criminals to operate in Australia and by eliminating vulnerabilities that organised criminals seek to exploit.

This report aims to inform the Australian community of the current and emerging organised crime threats that may directly or indirectly impact our nation. Members of the community are encouraged to report suspicious activities that could be linked to serious and organised crime by contacting their local police or by calling Crime Stoppers.

As serious and organised crime impacts all of us, it is important that we work together to discover, understand and respond to the threats of most harm to Australians and our national interests.

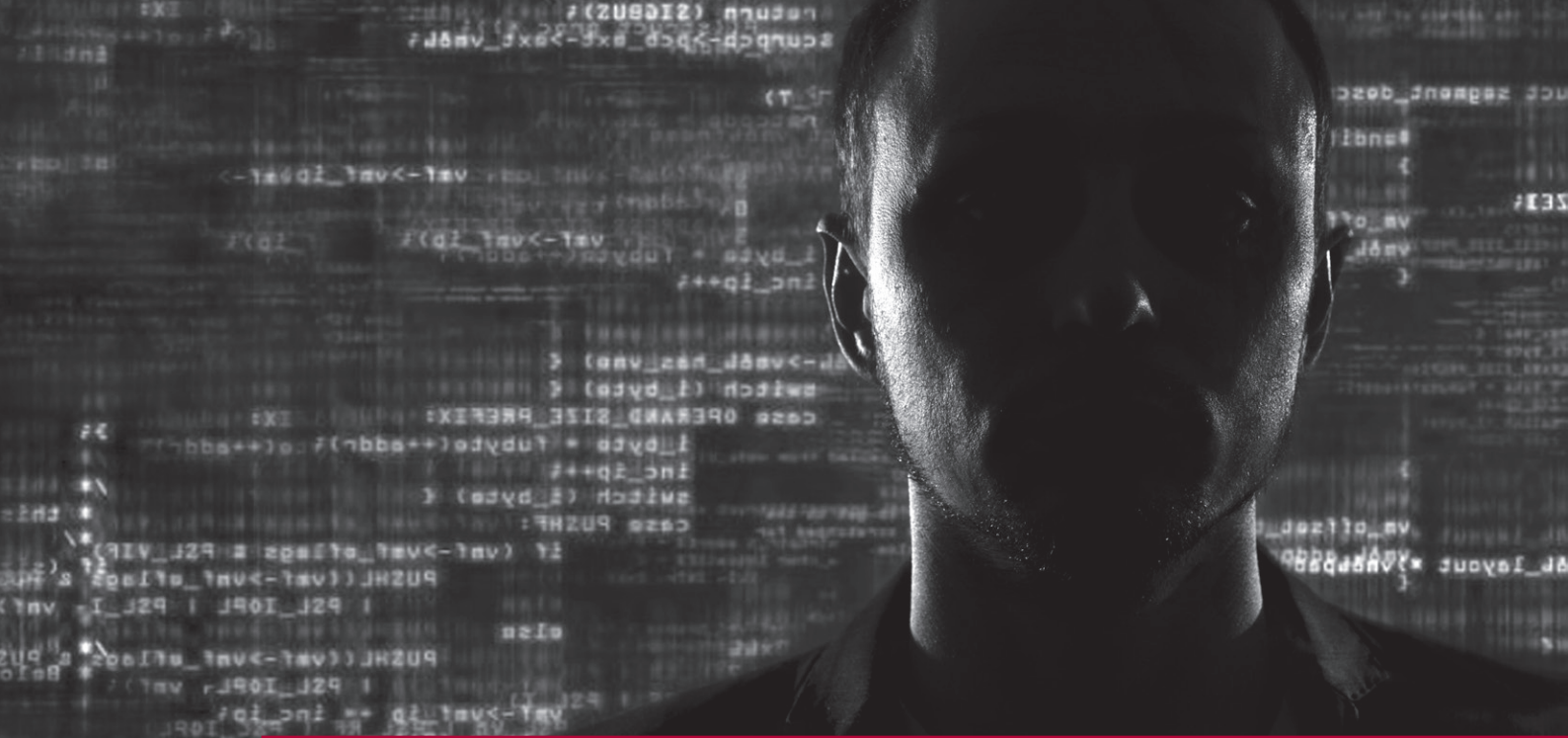


Chris Dawson APM
Chief Executive Officer
Australian Crime Commission

CONTENTS

INTRODUCTION	6
What does organised crime look like?	6
What are the key characteristics of organised crime?	7
How does organised crime affect us?	8
How are we responding?	9
 ENABLER ACTIVITIES	 11
Money laundering	12
Cybercrime and technology-enabled crime	16
Identity crime	20
Criminal exploitation of business structures	23
Public sector corruption	28
Violence	32
 ILLICIT COMMODITIES	 35
Illicit drug market overview	35
Methylamphetamine	36
Precursor chemicals	39
Cocaine	40
Heroin	42
Drug analogues and new psychoactive substances	43
MDMA	44
Cannabis	46
Illicit pharmaceuticals	47
Performance and image enhancing drugs	49
Anaesthetics	50
Tryptamines	51
Intellectual property crime	52
Firearm trafficking	56
Environmental crime	59

CRIMES IN THE MAINSTREAM ECONOMY	62
Card fraud	62
Revenue and taxation fraud	65
Illegal tobacco	68
Superannuation fraud	70
Investment and financial market fraud	72
Visa and migration fraud	75
 CRIMES AGAINST THE PERSON	 77
Human trafficking and slavery	77
Maritime people smuggling	78
Child sex offences	80
 THE OUTLOOK	 83
What will the organised crime environment look like over the next two years?	83



INTRODUCTION

What does organised crime look like?

The term 'organised crime' often conjures up stereotypical images—whether they be of the Mafia-type brotherhoods controlling large-scale crime rackets such as drug trafficking and money laundering, or of highly visible outlaw motorcycle gangs. In Australia, these depictions are still highly relevant, but there is also a less visible face of organised crime, which can be camouflaged within the community and harder to detect. For example, fraudulent investment schemes may be accompanied by glossy brochures, seminars or webinars and be promoted through slick websites, making them appear to be legitimate, even to the most financially literate members of the community. Many serious and organised crime groups present and operate as authentic businesses.

Advancing technologies and the online environment have presented new opportunities for organised crime to take advantage of our society's reliance on the Internet and automation. Cybercrime acts against individuals, businesses and governments, can be conducted from anywhere around the world, and can be easily carried out by individuals, organised crime groups or nation states. Defending the Internet against civilian and military intruders is now a high-priority global security problem. In November 2014, the Director of the United States National Security Agency told the House Intelligence Committee that some nation states had allegedly infiltrated the computers of critical industries (such as the electricity grid) to steal information and gather intelligence that could be used in the planning of an attack or to further advance malicious acts or interests, and warned of the ongoing risk of organised crime groups acting as proxies for nation states.

Organised crime groups involved in international drug trafficking are diversifying. No longer trading in one drug or commodity, some groups have begun trafficking in a number of commodities, including multiple drug types in the same shipment. Cooperation between organised crime groups is becoming more apparent, as is the intertwining of different types of criminal activities being undertaken by some organised crime groups.

Of particular significance in 2015 is the continuing threat of terrorism. The problem of Australians going abroad to fight is an emerging area of complexity for this country. As counter-terrorism efforts throughout Australia are enhanced, the linkages between terrorism and the broader organised crime and volume crime environments are being identified. These linkages include, but are not limited to, Australians who finance terrorist activities, Australians who leave Australia to support terrorist causes, and who may return to Australia with the intent of inflicting harm on the Australian community, or may be recruited by organised crime groups seeking the specialist skill sets they developed in foreign conflicts.

What are the key characteristics of organised crime?

In the current Australian environment, serious and organised crime is exploiting three key capabilities in particular:

1. The ability to conceal criminal activity by integrating into legitimate markets

Serious and organised crime has become interwoven with our economic, social and political environments. Although organised crime has continued to operate in traditional illicit markets, such as the illicit drug markets, it has been innovative in infiltrating legitimate industries to yield and launder significant criminal profits. In some instances, organised crime has sought to infiltrate specific industries to further its own activities, for example by setting up businesses within the transport, resources or investment sectors.

2. Technology and online capabilities

The uptake of new technologies by serious and organised crime reflects the adoption of these technologies by the general public. Serious and organised criminals have proven themselves adept at identifying and exploiting new and emerging technologies to facilitate their crime, to expand their reach, and to provide them with the anonymity and distance from their crime which makes it difficult for law enforcement to detect and identify them.

The ability to harness new and emerging technology to criminal ends is so fundamental to the success of high-level serious and organised crime entities that many employ specialists 'in-house', or contract their technology requirements to other groups who specialise in the provision of illicit technology services, or simply purchase ready-made malicious software to conduct criminal activity.

3. The globalisation of organised crime

Serious and organised crime is necessarily transnational and global in nature. Although individuals and groups involved in serious and organised crime will always vary in their capabilities, geographical reach and sophistication, there are groups, networks and individuals operating at an 'elite' criminal level and targeting illicit markets in a number of countries simultaneously. They are highly networked, highly professional and extremely well funded, and they operate with high-level specialist advice—including legal and financial advice—that allows them either to evade detection or to operate within the gaps in legislative and regulatory regimes internationally.

Transnational organised crime groups have the ability to adapt to market requirements and demands. They have capitalised on the high level of demand in Australia for methylamphetamine (particularly crystal methylamphetamine, or 'ice'). In the recent past, the methylamphetamine market has been dominated by domestic production. Significant production is still occurring domestically, but there has recently been a sharp increase in detections of methylamphetamine at the Australian border, suggesting that transnational organised crime groups have identified a gap in the market which they can fill.

How does organised crime affect us?

Organised crime affects the community in a number of ways—for example, there is a financial cost to governments in identifying, investigating, prosecuting and preventing it, and it can harm the national economy by pushing out legitimate business or eroding public confidence in the banking, finance or investment sectors.

Serious and organised crime also causes harms to the community that cannot be measured by a dollar value. For example, those affected by illicit drug use and their families may suffer severe physical and emotional anguish, and those who have lost their life savings to fraud may suffer not just financially but also psychologically from their loss. Organised revenue and taxation fraud, including the use of complex business structures and phoenixing,¹ deprives government of the funds needed to provide essential services such as hospitals, schools, roads and public transport.

In many cases, Australians are exposed to organised crime through the Internet. Cybercrime, predominantly the criminal use of malware, can target individuals and businesses, compromising their computer systems to steal data, or encrypting it and holding it to ransom. Individuals can have their banking credentials or their identity details stolen online and fraudulently used by a criminal, and Australians are falling victim to many online frauds, including 'online romance scams', with some people handing over up to A\$100,000 to fake love interests.

¹ Phoenixing occurs when a company goes into liquidation, leaving its debts behind, while the assets are shifted to a new entity that begins trading again, often under a similar name.

In late November 2014, the Australian Cybercrime Online Reporting Network (ACORN) was launched, allowing members of the public and small to medium businesses to report cases of cybercrime. It also provides the public with educational resources on how to detect cybercrime and avoid falling victim to increasingly sophisticated cybercrime methods. In the first quarter of 2015, more than A\$234 million of financial loss was reported via the ACORN.² This figure is based on values nominated by victims of cybercrime regarding the loss of data, money, goods and the compromise of personal information. Forty-one per cent of loss reported in the first quarter of 2015 resulted from online scams or fraud.

How are we responding?

Law enforcement and governments are actively responding to the threats posed by organised crime. Collaboration between government agencies, as well as with the private sector, is continually strengthening this response through new initiatives and improved relationships and information sharing.

The *National Organised Crime Response Plan 2015–2018* (the Response Plan) aims to enhance current strategies in place as a result of the *National Organised Crime Response Plan 2010–13*, as well as complementing other existing strategies—such as the *National Plan to Combat Cybercrime* and the *National Identity Security Strategy*—to harden Australia’s environment against organised crime.

The Response Plan provides a national platform to progress practical initiatives targeting the current key threats, where jurisdictions consider that national action can achieve maximum benefit. To meet the evolving and increasingly complex threat posed by serious and organised crime, our response requires a coordinated national approach that harnesses collective resources, capabilities, expertise and knowledge.

Effectively combating serious and organised crime will be dependent on law enforcement’s ability to operate in an increasingly interconnected and globalised financial environment, facilitated by the digital economy and international trade. This is a challenge faced by all nation states.

New international partnerships and information-sharing initiatives, such as the Five Eyes Law Enforcement Group,³ will facilitate targeted international law enforcement responses, innovative policy and legislative reform. Australia’s participation in international information-exchange forums will help improve our ability to discover, understand and respond to transnational serious and organised crime, including cybercrime, over the long term.

Ensuring strong border controls is a key factor in limiting the impact of organised crime in Australia. The National Border Targeting Centre (NBTC), established in 2013, brings together key law enforcement, border security and government policy bodies to develop more proactive, informed risk assessment responses to border threats to Australia. The NBTC enables increased domestic information sharing and also incorporates intelligence from international partner agencies.

² As these figures are self-reported, their accuracy has not been verified by law enforcement agencies at this time.

³ The Australian Crime Commission and the Australian Federal Police are the Australian representative members of the Five Eyes Law Enforcement Group which coordinates intelligence agencies from Australia, New Zealand, the United Kingdom, the United States and Canada.

Further, the increasingly complex nature of the serious and organised crime business model requires effective partnerships between law enforcement and industry to achieve holistic targeting of organised crime activities in Australia. Joint agency task forces that target the exploitation of alternative remittance services by organised crime—for example, the Eligo National Task Force—work closely with industry participants to identify criminal elements exploiting their industry and collaboratively devise strategies to help prevent such exploitation.

Preventative partnerships are also crucial. The Australian Cyber Security Centre (ACSC) unites cyber security capabilities from across the Australian Government into a collaborative hub to share information between member agencies and the private and public sectors to combat cyber-security threats. The ACSC also houses CERT Australia,⁴ which deals with large business and government cyber-security incidents. Small businesses and the public are able to report incidents through the ACORN, which has a convenient online reporting system. The information collected by the ACORN and the ACSC (and its integrated assessment agencies) provides the government with a contemporary understanding of the changing cyber-security landscape and how to harden the environment to protect Australia.

The criminal activities of gangs, particularly outlaw motorcycle gangs (OMCGs), consistently attract public attention. The Australian Gangs Intelligence Coordination Centre (AGICC) brings together law enforcement, border security and government departments with the aim of delivering operational intelligence, strategic intelligence, and disruption and prevention strategies. This helps to build a better understanding of the gang environment in Australia and inform appropriate response options. The AGICC also delivers a dedicated intelligence collection capability for the Australian Federal Police (AFP)-led National Anti-Gangs Squad.⁵

Engagement with the public is crucial to success in combating organised crime; without the help of the public in identifying and reporting suspected criminal activity, the environment will never be completely hardened against it.

⁴ CERT Australia is the national Computer Emergency Response Team.

⁵ The National Anti-Gangs Squad is operational in New South Wales, Victoria, Queensland and Western Australia.



ENABLER ACTIVITIES

The Australian Crime Commission has identified six illicit activities as being ‘key enablers’ for organised crime. Those activities are:

- Money laundering
- Cybercrime and technology-enabled crime
- Identity crime
- Criminal exploitation of business structures
- Public sector corruption
- Violence.

These activities are classified as ‘enablers’ because they each have unique roles in enabling or facilitating organised crime, but are not an end in themselves—that is, money laundering would not be necessary if the crime from which illicit profit had been made had not been committed, necessitating concealment of the proceeds of that crime. Similarly, the theft of identity documents would pose little threat if those documents were not intended to be used to commit offences.

Activities such as money laundering, identity crime, corruption and violence contribute to the effectiveness of other types of organised crime. Although not all of the enablers are present in every illicit market, enablers can work in unison, with any one organised crime group using several enablers at once. Corruption can be used to facilitate, or to hide, the use of other enablers.

Importantly, enablers are also unique in that any impacts of law enforcement, regulatory, legislative or policy activity that are felt within the enabling activities—such as closing loopholes in financial reporting systems to inhibit money laundering—have the potential to resonate through all of the illicit markets in which those enabling activities are present. For example, should law enforcement capability to identify, trace and prosecute cybercrime and technology-enabled crime be enhanced, all of those markets that rely on technology to perpetrate crime would be significantly affected.

Money laundering

Introduction

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.

Money laundering diminishes tax revenue, weakens government control over the economy, and can undermine the integrity of Australia's financial system and other industry sectors.⁶

As a result of concerted law enforcement attention being focused on money laundering in Australia, much has recently been learned about the way in which the proceeds from the importation and sale of illicit commodities are laundered out of, and within, Australia. For example, intelligence arising from the investigations carried out by the Eligo National Task Force has revealed that money laundering associated with the proceeds of crime derived from illicit commodities markets in Australia is increasingly carried out with the assistance of professional advisers and specialist globalised money laundering networks (see the case study on page 13).

Current situation

For organised crime operating in Australia, money laundering is increasingly a transnational enterprise, with the proceeds of crime generated in Australia typically being put through an international money laundering cycle. The complex transnational nature of money laundering has led organised crime to more often employ the services of professional money laundering syndicates.

Unlike the proceeds from the trafficking and sale of illicit commodities—which are often realised in the form of cash—the profits generated by financial crime are likely to be already placed⁷ in a financial system or market, making it easier to electronically transfer these funds quickly around the world through a complex series of accounts designed to conceal beneficial ownership.

In the case of the proceeds of financial crime, the illicit funds are likely to be 'washed' by means of a complex series of funds transfers through multiple jurisdictions. These transfers are likely to include structured funds transactions, complex business structures and Alternative Banking Services.⁸

6 Australian Transaction Reports and Analysis Centre 2011, *Money laundering in Australia*, AUSTRAC, Sydney.

7 The money laundering cycle typically consists of three stages: placement, layering and integration. Placement occurs when illicit funds or assets are introduced into the formal financial system. Layering involves moving, dispersing or disguising illegal funds or assets to conceal their true origin. Integration refers to the movement of illicit funds back into the legitimate economy.

8 An Alternative Banking Service includes an online banking interface, which sits above and coordinates one or multiple bank accounts, supported by company structures, in various international locations.

CASE STUDY

ELIGO NATIONAL TASK FORCE

The Eligo National Task Force was established by the Australian Crime Commission (ACC) Board in December 2012 to take coordinated collective action against high risk alternative remittance and informal value transfer systems¹ being used by serious and organised crime to reduce their adverse impact on Australia. The Task Force combines the capabilities of the ACC, the Australian Federal Police, the Australian Transaction Reports and Analysis Centre, state and territory law enforcement and overseas law enforcement partners.

The Eligo National Task Force has yielded significant insights into the way in which the proceeds from the trafficking and sale of illicit commodities are laundered, particularly by discovering new methods of laundering proceeds of crime. As well as increasing our knowledge of money laundering processes, the Task Force has also gained a significant understanding of how alternative remittance systems work in different cultures and countries.

The interconnectedness of money laundering networks and the variety of laundering methodologies that have been identified demonstrate a truly organised and global system of criminal business.

Examples of international money laundering methodologies identified by the Eligo National Task Force investigations are informal value transfer systems, trade-based money laundering² and structuring.

A significant money laundering modus operandi that has been identified in Eligo investigations is the use of offshore money laundering superfacilitators. Intelligence has shown that some criminal groups using alternative remittance services have their laundering activities coordinated by offshore money laundering superfacilitators or controllers, who direct the activities of 'cash collectors' in multiple countries, including Australia. These cash collectors are used to place money into the alternative remittance system, where offshore superfacilitators will manage the money laundering process (see Figure 1).

Since its commencement, the Eligo National Task Force has undertaken significant operational activity, culminating in the disruption of several global money laundering and drug networks. In conjunction with partner agencies, Task Force investigations to date³ have resulted in:

- A\$65.9 million in cash seized
- A\$925.7 million in estimated street value of drugs and precursors seized
- 289 persons arrested on 673 charges
- A\$46 million in assets restrained
- 52 serious and organised criminal networks or groups disrupted
- 284 new targets identified that were previously unknown to law enforcement.

Prevention is also a focus of the Task Force, which will aim to harden the alternative remittance services sector against exploitation by organised crime. The Task Force is working with industry to identify areas of vulnerability and drive initiatives aimed at preventing further such exploitation.

1 Informal value transfer systems are global networks for financial transactions that involve transferring the value of currency without necessarily physically relocating it. For further information, please refer to the ACC website: <https://www.crimecommission.gov.au/sites/default/files/IVTS%20D6.pdf>

2 Trade-based money laundering allows organised crime groups to move funds by disguising it as legitimate trade. For further information, please refer to the ACC website: <https://www.crimecommission.gov.au/sites/default/files/Trade%20Based%20D5.pdf>

3 As at 31 March 2015.

MONEY LAUNDERING 101

HOW IT WORKS

MONEY LAUNDERING:

The basic motivation behind most crime is to make money. If criminals want to use that money it needs to appear to have come from legitimate sources. This means they need to 'clean' or 'launder' it. There is no single method of laundering money. Money launderers have shown themselves to be imaginative, and utilise a variety of methods to get around counter-measures designed to identify and stop this activity.

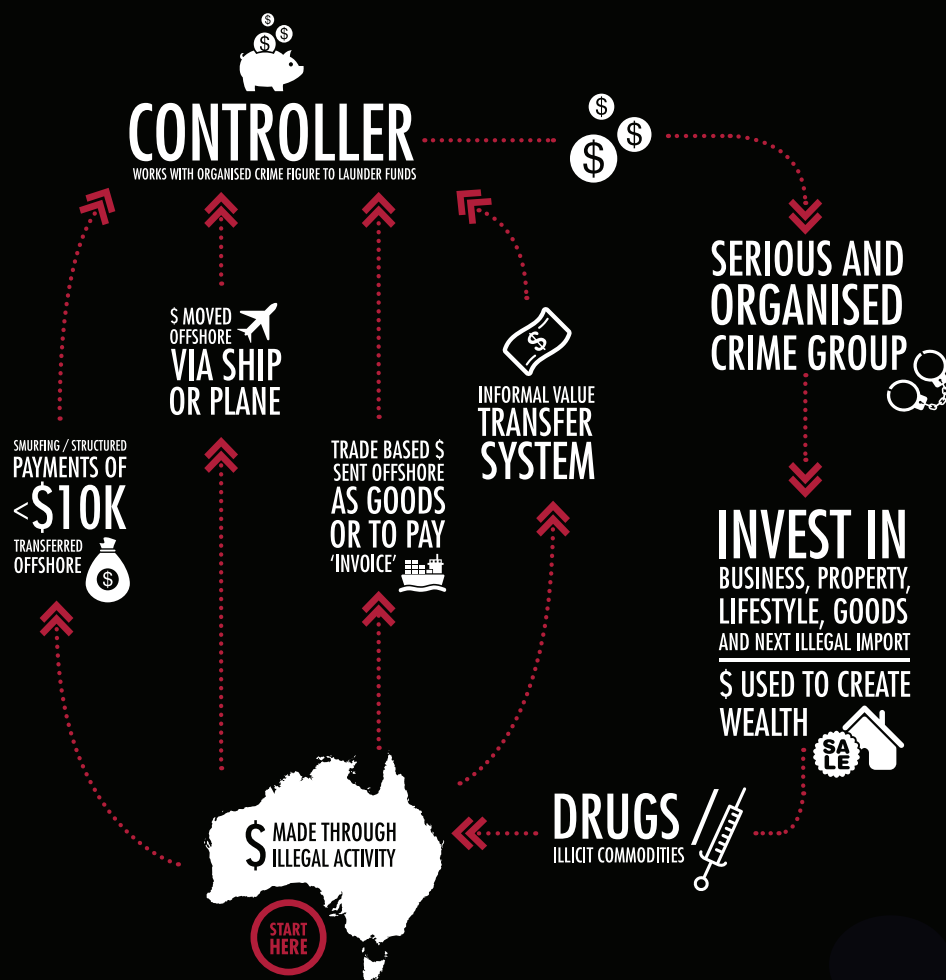


Figure 1: A money laundering methodology identified in Eligo National Task Force investigations

Current situation (continued)

The Eligo National Task Force has identified the increasing use of professional money laundering syndicates by serious and organised crime groups, primarily those involved in trafficking illicit drugs. However, those involved in serious and organised financial crime probably possess, or have access to, sufficient expertise to support laundering the proceeds of their crimes independently of professional money laundering syndicates.

Globalisation and technology have led to the development of a financial system that permits the rapid transfer of value around the world, with those responsible for the movement of the funds able to orchestrate transfers with relative anonymity from behind a computer screen.

Money laundering is carried out through a diverse range of financial markets and by a variety of methods. Some examples of how organised crime can exploit financial markets and/or methodologies to launder the proceeds of crime are:

- The securities or share market is attractive for money laundering as it offers a diverse and complex suite of investment vehicles across domestic and international markets. The securities market can afford investors a high level of anonymity, particularly when trading through professional brokers. The reporting of suspicious financial transactions in the securities market remains relatively low.

- Foreign exchange trading—or ‘forex’ trading—involves the swapping or trading of one currency for another, with a profit or loss being made when one currency increases or decreases in value. Foreign exchange trading is likely to be attractive to those engaged in money laundering as such markets are highly liquid and operate internationally, enabling high levels of anonymity.
- Virtual currencies, such as Bitcoin, continue to be used as a means of transferring value online and without reliance on any financial institutions to facilitate the transaction.
- Complex offshore and third-party business structures are used to disguise wealth and inhibit law enforcement and regulatory bodies in the collection of evidence of illicit activities.
- 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.
- Investment in high-value commodities—such as real estate, precious stones, art, antiques and gold—can be used by organised crime entities to place and integrate illicit funds into the legitimate economy. For example, organised crime can invest in Australia’s real-estate sector, with the investments subsequently sold and the proceeds from the sale integrated into the formal banking system.

Serious and organised crime groups are increasingly employing financial technology platforms to advance their criminal activities. These Alternative Banking Services may be used for large-scale frauds and avoidance of taxation obligations. They require a high degree of financial acumen to establish and manage, in order to successfully disguise funds transfers outside the regulated environment. The ability of those involved in serious and organised crime to launder money allows for re-investment of the proceeds of crime, and therefore the perpetuation of criminal enterprise. Money laundering activities also have the potential to cause reputational damage to financial institutions or, in more severe scenarios, to undermine the soundness and stability of financial institutions and systems, discourage foreign investment, distort international capital flows and damage diplomatic relations. A government’s inability to inhibit the laundering of illicit funds may lead to a perception that it is legislatively or administratively ineffectual. Such reputational damage can discourage investment, as corporations and foreign governments seek to distance themselves from nation states ‘tainted’ by money laundering.

Further harm may be caused by the methods that are used to launder money. The primary goal of money laundering is to give illicit money the appearance of legitimacy. Consequently, funds are likely to be invested not on the basis of likely returns, but in businesses or schemes that provide the greatest chance of concealing the origins of the money. This can erode the ‘level playing field’ on which legitimate businesses compete, distort markets and enhance the economic power of organised crime.

Cybercrime and technology-enabled crime

Introduction

The threat to Australia from cybercrime and technology-enabled crime perpetrated by international and domestic organised crime groups is significant. Technology, computers and the Internet are now integral parts of everyday life, used for purposes such as Internet banking, online shopping, email and communication through social media. Organised crime has identified and seized the opportunity to exploit for financial gain Australians' use of digital systems and the Internet. There are a diverse range of devices that can be exploited by criminal actors, including computers, mobile phones and point of sale (POS) systems. Potential victims include government, critical infrastructure agencies, industry, businesses and the public.

The 2013 Norton Report estimates that cybercrime affected five million Australians in the previous 12 months and cost Australians A\$1.06 billion.⁹ This is likely to be an underestimation, as it is only based on adult individuals affected and does not consider the cost to industry and government. It has been reported that the most costly cybercrimes affecting Australian companies are those caused by malware, distributed denial of service and malicious insiders.¹⁰ As mentioned in the introductory chapter of this document, more than A\$234 million worth of financial loss was self-reported by victims of cybercrime to the Australian Cybercrime Online Reporting Network (ACORN) in the first quarter of 2015.¹¹ If similar figures continue to be reported each period, this would equate to A\$936 million over one year. It is important to note that this estimate would only account for losses affecting members of the public and small to medium businesses.

Current situation

In Australia, cybercrime and technology-enabled crime refers to criminal acts involving the use of computers or other information and communications technology (ICT), or targeted against computers or other ICT. The term 'cybercrime and technology-enabled crime' is defined as:

- Crimes directed at computing or other ICT, such as unauthorised access to, modification of or impairment of electronic communications or data. The international community refers to this as pure cybercrime.
- Crimes in which computers or ICT are an integral part of the offence, such as online fraud, online identity theft and the online distribution of child exploitation material. The international community refers to this as facilitated cybercrime.

9 Symantec 2013, '2013 Norton Report: Total cost of cybercrime in Australia amounts to AU\$1.06 billion', media release, 13 October 2013, viewed 19 January 2015, <http://www.symantec.com/en/au/about/news/release/article.jsp?prid=20131015_01>.

10 Ponemon Institute 2013, *2013 Cost of Cyber Crime Study: Australia*, Ponemon Institute, Traverse City, Michigan, October 2013.

11 As these figures are self-reported, their accuracy has not been verified by law enforcement agencies at this time.

Australia has a large and increasing number of Internet users, all of whom are potential victims of cybercrime. At the end of June 2014, in Australia there were more than 12.4 million Internet subscribers and almost 20.6 million subscribers to mobile services with an Internet connection.¹² Mobile devices are just as vulnerable to attack as traditional devices such as desktop computers and laptops; however, many mobile users do not give the same degree of consideration to the security of these devices as they do to computers. The 2013 Norton Report revealed that 57 per cent of Australian mobile device users were not aware of security options for mobile devices, leaving their devices susceptible to attack.¹³

Cybercrime committed against Australians is assessed to be largely carried out by individuals and organised crime groups based offshore. However, increasing awareness of, and access to, online criminal forums and marketplaces (often referred to as 'darknets') is also enabling Australia-based criminal actors to share information and to trade illicit services and commodities internationally. Cybercrime toolsets, predominantly malicious software ('malware'), are available for purchase and ongoing service support is provided. This widens access to a previously highly technical capability to any actor with an average proficiency and a criminal intent to pursue an illicit profit.

Some malware can operate without detection by anti-virus software. Malware is sophisticated, intelligent, versatile and available, and is affecting a broader range of targets and devices.¹⁴ The development of malware is maintaining pace with the modern technological environment, constantly evolving to counter new security mechanisms so that it maintains effectiveness. ZeroAccess is an example of a recent strain of highly resilient malware that has compromised a large number of Australian devices and continues as a persistent threat (see the case study on page 18).

Organised Crime in Australia 2013 reported on an increase in 'ransomware' campaigns against computers in Australia and around the world. There are variations on the ransomware campaign methodologies and themes. Some ransomware encrypts all files and will not allow access until a fee has been paid to decrypt them. Other types of ransomware disable user input, indicate that files have been encrypted and activate the webcam in an effort to convince the user that their system is under real-time surveillance. This is reinforced by an accompanying message (often purporting to be from a law enforcement or government agency) claiming that the computer had been used in illegal activity and demanding payment of a 'fine'. These types of cybercrime campaigns have increasingly affected Australian systems over the last two years (see the case study on page 19).

12 Australian Bureau of Statistics 2013, *Internet activity Australia, June 2014*, Cat. no. 8153.0, ABS, Canberra, viewed 3 October 2014, <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/>>.

13 Symantec 2013, '2013 Norton Report: Total cost of cybercrime in Australia amounts to AU\$1.06 billion', media release, 13 October 2013, viewed 19 January 2015, <http://www.symantec.com/en/au/about/news/release/article.jsp?prid=20131015_01>.

14 Europol European Cybercrime Centre EC3 2014, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, viewed 27 November 2014, <<https://www.europol.europa.eu/iocata/2014/>>.

CASE STUDY

ZEROACCESS

Between October and December 2014, 'ZeroAccess' malware reportedly compromised an average of 4,000 Australian devices per day.¹ The ZeroAccess botnet² is a large collection of infected computers linked by peer-to-peer infrastructure³ being directed to carry out bitcoin mining⁴ and click fraud⁵ on victims' computers.

ZeroAccess is highly commercialised and highly profitable malware with a 'pay-per-install' incentive that has contributed to its growth. The amount paid is based on the country in which the installation occurs, with installations on Australian computers earning US\$75.⁶

ZeroAccess uses an advanced method of self-protection by disabling any security tool trying to detect and remove it.⁷ It also targets a diverse range of devices. It affected POS systems in 60 Pizza Hut stores in Australia over a 12-month period in 2014. Trade was halted for up to two hours per incident and, in some cases, stores were offline for an entire day because infected machines required re-imaging.⁸

Despite overseas law enforcement interdiction, ZeroAccess has proved resilient. In December 2013, Europol, the Federal Bureau of Investigation and Microsoft worked together to disrupt the ZeroAccess botnet but reported that they were unable to completely disrupt it because of its complexity.⁹

ZeroAccess remains a high threat in Australia, being one of the malware types most commonly reported by Australian victims.¹⁰ Although its current functions are bitcoin mining and click fraud, it has the potential to be used for other types of cybercrime activity.

- 1 Australian Communications and Media Authority, *AISI malware statistics*, viewed 19 December 2014, <<http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/aisi-malware-statistics-1>>.
- 2 A botnet is a large network of infected computers owned by individuals who are unaware that their computers are compromised. Botnets are controlled remotely by a command control (C2) server.
- 3 Peer-to-peer infrastructure is a network of computers, usually connected through the Internet, that enables propagation of communications among the peers, without the need for a central server.
- 4 Bitcoin mining is a legitimate activity and is integral to the bitcoin system. As bitcoin is not centrally controlled, mining is the process by which transactions are validated in the bitcoin blockchain. It involves using a computer to solve complex cryptographic algorithms that, when solved, close off a block in the chain, thus protecting it from being changed and reinforcing the legitimacy of transactions. When a 'miner' solves a problem, they are rewarded with bitcoin.
- 5 Click fraud abuses pay-per-click advertising to make money through fraudulent clicks. Pay-per-click advertising is a major industry, generating billions of dollars per year. A hosting website places an advertiser's ad on their website and each time the ad is clicked the advertiser pays the hosting website. A cybercrime actor can make money if they can generate fraudulent clicks on an advertisement and are also the hosting website that receives payment.
- 6 Wyke, J 2012, *Sophos Technical Paper: The ZeroAccess botnet—mining and fraud for massive financial gain*, Sophos, September 2012, viewed 19 December 2014, <http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf>.
- 7 McAfee for Business, *Threat Intelligence: ZeroAccess.a*, viewed 27 November 2014, <<http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=562354>>.
- 8 Vijay 2014, 'Pizza Hut Australia point of sales hit with ZeroAccess rootkit malware for over a year', *Tech Worm*, 10 November 2014, viewed 19 December 2014, <<http://www.techworm.net/2014/11/pizza-hut-australia-point-sales-hit-zeroaccess-rootkit-malware-year.html>>.
- 9 Kirk, J 2013, 'ZeroAccess click-fraud botnet disrupted, but not dead yet', *Computer Security Online*, 6 December 2013, viewed 19 December 2014, http://www.cso.com.au/article/533664/_zeroaccess_click-fraud_botnet_disrupted_dead_yet/; Europol 2013, 'Notorious botnet infecting 2 million computers disrupted', media release, 5 December 2013, viewed 19 January 2015, <<https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted-0>>.
- 10 Australian Communications and Media Authority, *AISI malware statistics*, available at <<http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/aisi-malware-statistics-1>>.

CASE STUDY

TORRENTLOCKER

First identified as a new variant of malware in February 2014, TorrentLocker is designed to avoid known virtual malware testing environments and to employ novel techniques to ensure that detection and evaluation are difficult.¹ Once initiated, certified encryption protocols protect the malware files on the victim's computer.²

During 2014, TorrentLocker was distributed by means of spam emails targeting 13 countries but, as identified by the Australian Crime Commission (ACC), initially it only targeted Australia. The ransom message delivered to Australian computers listed the ransom fee in Australian dollars and required the victim to purchase bitcoins from specified Australian bitcoin websites and send the payment to the bitcoin address provided.³

As at December 2014, it was estimated that TorrentLocker had infected more than 39,000 systems worldwide and that 570 of them (less than 2 per cent) had paid the ransom.⁴ It is estimated that the total ransom money paid to that date was worth between US\$292,700 and US\$585,401.⁵

TorrentLocker used the branding of a number of trusted and well-recognised Australian corporations. The misappropriation of business names and the counterfeiting of legitimate brands harm the reputation of these businesses, may destroy the loyalty of established customers and will cost businesses financially if they seek remediation. The onus is then on the affected business to expend time and resources in educating its customer base about scams that exploit its business identity. One prominent Australian corporate victim whose brand has been exploited by the ransomware infection campaign estimates that since mid-2014 its response to TorrentLocker has cost A\$185,000. This response has included monitoring, takedown actions against malicious domains, and brand protection.

The ACC's detailed understanding of the TorrentLocker malware resulted in the ACC proving that other allied countries were also being targeted by TorrentLocker, albeit not to the same extent as Australia.

1 Léveillé, MM 2014, 'TorrentLocker ransomware in a country near you', *welivesecurity*, December 2014, viewed 11 February 2015, <www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf>.

2 *ibid.*

3 Hummel, R 2014, 'Analysis of "TorrentLocker"—a new strain of ransomware using components of CryptoLocker and CryptoWall', *iSIGHT Partners*, 15 August 2014, viewed 11 February 2015, <<http://www.isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/>>.

4 Léveillé, MM 2014, 'TorrentLocker ransomware in a country near you', *welivesecurity*, December 2014, viewed 11 February 2015, <www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf>.

5 *ibid.*

The Internet is an integral part of our everyday lives, with our reliance on it continuing to grow. The automation of industry, government departments, businesses and banking presents risks from cybercrime at a systemic and individual level. The Office of the Australian Information Commissioner reports that the potential for personal information to be misused, lost or inappropriately accessed, modified and disclosed is increased by greater collection of personal information in the online environment and reliance on electronic and online records.¹⁵ Both businesses and government have a business requirement to collect and store customer information. However, this information is appealing to criminals and is at risk of exploitation for criminal deployment of malware, hacking and malicious insider exploitation. For example, in December 2014, an Australian hacker broke into an online travel insurance provider's systems, stealing the personal details of about 770,000 customers.

Cybercrime motivated by political or other issues (colloquially known as 'hacktivism') continues to be detected around the world. In late 2014 and early 2015 there were a number of high-profile instances of issue-motivated cybercrime. These included the cybercrime acts against Sony Pictures, resulting in the release of employee personal information, emails and unreleased films, and cybercrime acts against the United States Central Command's Twitter feed.

Identity crime

Introduction

Identity crime is a generic term that describes activities or offences in which a perpetrator steals a person's identity or uses a fabricated, manipulated, stolen or otherwise assumed identity to facilitate the commission of a crime.¹⁶

Identity crime, though under-reported, is among the most prevalent crime types. An increased reliance on personal identity information (PII) in online services, along with the exploitation of technology by criminals, has seen identity crime become one of the most pervasive crime types in Australia.

Identity crime acts as an enabler of a wide range of other organised criminal activities, particularly the facilitation of financial crimes and money laundering, which can result in significant harm to individuals, business, the government and the economy.

¹⁵ Office of the Australian Information Commissioner 2015, *Guide to securing personal information*, January 2015, viewed 22 January 2015, <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security>>.

¹⁶ Adapted from Australasian Centre for Policing Research 2006, *Standardisation of definitions of identity crime terms: a step towards consistency*, viewed 5 November 2013, <<http://www.anzpaa.org.au/anzipire/acprpublications>>.

Current situation

A community survey conducted by the Australian Institute of Criminology in 2013¹⁷ found that 9.4 per cent of respondents reported having their personal information stolen or misused in the previous 12 months. Five per cent of respondents (equivalent to about 1 million people throughout Australia) reported that they suffered financial losses as a result. This rate of victimisation is higher than for most other types of personal and theft-related crimes.

A report published by the Attorney-General's Department in 2014 estimated that the total economic impact of identity crime on Australia was at least A\$1.6 billion per year.¹⁸ The United Kingdom's Fraud Prevention Service (known as CIFAS) has found that 49 per cent of all fraud was identity fraud and that over 60 per cent of all fraud involved some form of identity-related crime.¹⁹

However, accurate measurement of the full extent of identity crime offences, their impact and the extent to which serious and organised crime groups are involved is limited by a number of factors:

- The cross-jurisdictional nature of identity crime creates difficulties in determining which jurisdiction an offence has been committed in. For example, PII could be stolen in one country and used to commit an offence in another. The difficulties are exacerbated by the increasing use of cloud computer storage, allowing businesses to outsource their information technology services and applications to a third party, which may be located interstate or offshore.
- Identity crime-related legislation and its application vary across police jurisdictions. Identity-related crimes are often recorded and/or prosecuted using other types of offences such as fraud, particularly where these other offences attract higher penalties.
- Identity crime-related incidents are not always reported. Victims may not be aware that their PII has been compromised, or may report the offence to their financial institution rather than the police.
- At a corporate level, businesses may be reluctant to report losses from identity crime to avoid a loss of confidence in the business.
- The impact of PII theft may not be evident for a number of years, as PII may be stored for future use. Consequently, law enforcement agencies may have trouble identifying the original source and the time of the breach.
- Identity crime as an enabler provides key support to much broader criminal activities, such as money laundering and drug trafficking, meaning that the harm resulting from the identity-related crime component is difficult to measure.

¹⁷ Smith, RG & Hutchings, A 2014, *Identity crime and misuse in Australia: results of the 2013 online survey*, Australian Institute of Criminology Reports, Research and Public Policy Series no. 128, AIC, Canberra.

¹⁸ Attorney-General's Department 2014, *Identity crime and misuse in Australia: key findings from the National Identity Crime and Misuse Measurement Framework Pilot*, AGD, Canberra.

¹⁹ CIFAS 2014, *Fraudscape: depicting the UK's fraud landscape*, March 2014, viewed 20 February 2015, <https://www.cifas.org.uk/research_and_reports>.

Stolen or false identities can be used by criminals to perpetrate frauds and to establish business structures and companies through which to facilitate crimes such as money laundering. Identity crime has also been used to commit welfare, tax and other fraud against government agencies, to gain unauthorised access to sensitive information or facilities, to conceal other criminal activities such as drug trafficking and procuring child exploitation material, and even to facilitate the commission of terrorist acts.

Fraudulent identity credentials can be obtained for amounts ranging from about A\$80 for Medicare cards, A\$350 for drivers licences, A\$1,500 for a genuine Australian passport altered by a professional document forger, to as much as A\$20,000–\$30,000 for a legitimately issued passport with fraudulent identity details.²⁰

These types of primary and secondary identity documents can then be used to support criminal activities such as credit card fraud, bank fraud and money laundering (see the case study on page 23).

Organised crime continues to adapt its identity crime methodologies to exploit technological changes. The use of wireless technology for credit card payments, or ‘tap and go’, is enabling the reading of PII on various kinds of identity and credit cards. An industry survey found that over half of Australian adults use public or unsecured Wi-Fi, with a quarter of these people using it to shop online (27 per cent) or to access their bank accounts (25 per cent).²¹ As well, smartphones and related devices that send emails and access online social networking sites provide organised crime with a single, and often unsecured, avenue through which to target the PII of individuals. Those using poor security practices—such as providing personal information to unknown sources and using devices without adequate anti-virus software—are most likely to fall victim to these identity crime methodologies.

There is also a risk that organised crime may seek to corrupt or compromise individuals employed in sectors with access to large datasets of PII. Through these individuals, organised crime may be able to access PII for use in other criminal activities.²²

Use of the Document Verification Service (DVS) by government agencies and private sector organisations is increasing and over time this could be expected to help reduce the use of fake or stolen identity documents in the community. The DVS enables organisations to verify information they are presented on identity documents against the records of the document issuing agency, in real time through a secure online system.

It is important that service delivery agencies undertake robust security and fraud risk assessments, in consultation with law enforcement and other relevant agencies, to help ensure that these risks can be managed effectively.

20 Attorney-General's Department 2014, *Identity crime and misuse in Australia: key findings from the National Identity Crime and Misuse Measurement Framework Pilot*, AGD, Canberra.

21 Symantec 2013, *2013 Norton Report—country report: Australia*, viewed 2 February 2015, <<http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-australia.pdf>>.

22 Attorney-General's Department 2014, *Identity crime and misuse in Australia: key findings from the National Identity Crime and Misuse Measurement Framework Pilot*, AGD, Canberra.

CASE STUDY

SYDNEY-BASED IDENTITY FRAUD GROUP

In February 2015, a joint agency investigation codenamed Operation Mera,¹ based in New South Wales (NSW), arrested four people in relation to their alleged involvement in a fraudulent identification manufacturing operation.

The group's alleged activities were reported to have been first identified when the Australian Customs and Border Protection Service found 5,000 NSW drivers licence holograms concealed in a package imported from China.

Search warrants executed at a number of locations have reportedly seized 'computer equipment, printers, card cutters, thousands of blank cards, holograms for licences and credit cards, electronic card templates, card readers, and fraudulent identity documents in various states of manufacture from both Australia and overseas'. As well, more than 100 mobile phones, cash and false identity documents were also allegedly located.

¹ New South Wales Police Force 2015, 'Joint agency investigation shuts down fraudulent identity manufacturing operation', media release, 26 February 2015, viewed 26 February 2015, <http://www.police.nsw.gov.au/news/latest_releases?sq_content_src=%2BdXJsPWh0dHBzJTnBJTJGJTJGZWJpenByZC5wb2xpY2UubnN3Lmdvdi5hdSUyRm1lZGlhJTJGNDQ1OTEuaHRtbCZhbGw9MQ%3D%3D>.

Although most identity crime against individuals involves relatively small financial losses, in some cases these losses can be very significant. Also, being a victim of identity crime can also involve significant non-financial impacts, including reputational damage as well as emotional and psychological harm.

Criminal exploitation of business structures

Introduction

The criminal exploitation of business structures involves both the use of unlawful business practices and the deliberate structuring of businesses for purposes including the following:

- to conceal the criminal infiltration of an industry
- to generate and/or conceal illicit profits
- to gain an unfair advantage over competitors by expanding market share.

This may be through the exploitation of simple and complex business structures, through the practice of fraudulent phoenixing,²³ 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.

The criminal exploitation of business structures by organised crime results in financial gains for criminals and financial losses to the Australian economy. It may also affect public confidence and the perceived legitimacy and validity of business and company regulatory processes and requirements.

Current situation

Simple business structures

The simplest form of business structure—the sole trader—makes up the highest proportion of registered businesses in Australia. This type of structure is predominantly used to operate businesses in cash-intensive industries, and these industries are attractive to organised crime because of the relatively untraceable nature of cash transactions and the opportunity to commingle illicit and legitimate funds. Organised crime groups can create multiple sole trader entities in order to facilitate tax evasion or money laundering activities.

Organised crime can also exploit business and company registration processes through the use of identity crime, fictitious names or the placement of ‘straw’ or nominee proprietors or company office holders. Law enforcement investigations have typically shown organised crime involved in operating ‘cash’ businesses.

Complex business structures

There is continued use of complex ownership and control structures, often involving separate entities from multiple jurisdictions, to effectively hide the ultimate beneficial ownership of the underlying entity and any asset holdings. Complex business structures, particularly trusts with international connections, are mainly used to commit large-scale revenue and taxation fraud and facilitate money laundering. Complex business structures are exploited by organised crime to facilitate circumvention of *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* reporting requirements, to establish complex business structures that create opacity of wealth, to set up offshore structures used to channel funds from Australia, or to hide wealth for the purposes of evading taxation.

Project Wickenby²⁴ 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.

²³ Phoenixing occurs when a company goes into liquidation, leaving its debts behind, while the assets are shifted to a new entity that begins trading again, often under a similar name.

²⁴ Project Wickenby is a cross-agency task force designed to strengthen national law enforcement and Australian Taxation Office (ATO) compliance activities against taxation fraud. Led by the ATO, Project Wickenby includes the Australian Crime Commission, the Australian Federal Police, the Australian Securities and Investments Commission, the Attorney-General's Department, the Australian Transaction Reports and Analysis Centre, the Australian Government Solicitor and the Commonwealth Director of Public Prosecutions.

Also, transnational ‘cold-calling’ investment fraud activity²⁵ is facilitated by the ease with which organised crime is able to develop sophisticated offshore business structures that effectively protect and insulate against law enforcement and regulatory identification and oversight.

Fraudulent ‘phoenix’ activity

Fraudulent ‘phoenix’ activity occurs when a company goes into liquidation, leaving its debts behind, while the assets are shifted to a new entity that begins trading again, often under a similar name. This deliberate practice is used to avoid paying the company’s creditors and its taxation liabilities to the Australian Taxation Office (ATO). The Fair Work Ombudsman released a research report in 2012, prepared by PricewaterhouseCoopers and titled *Phoenix activity: sizing the problem and matching solutions*,²⁶ which estimated that the annual cost of fraudulent phoenix activity in Australia is between A\$1.78 billion and A\$3.19 billion. This figure represents a combination of unpaid wages and other employee entitlements, losses to businesses in the form of unpaid debts and non-provision of services, and loss of government revenues.

Intelligence shows that fraudulent phoenix activity typically occurs in the small business sector (companies with fewer than 20 employees). Those industries in which phoenixing most commonly occurs include labour hire, cleaning, security, building and construction (particularly property development), manufacturing and retail (see the case study on page 26). A common methodology used to facilitate this activity is to register companies using non-existent directors or third-party/nominee directors.

The Australian Securities and Investments Commission (ASIC) reports that, during the financial year 2013–14, the company directors of 1,400 companies and 2,500 individuals in the building and construction, labour hire, transport, security and cleaning industries were targeted because of their history of failed companies.²⁷ During the 2012–13 financial year, ASIC reported that the construction industry had the largest number of company failures, with 2,245—or 24 per cent—of total failures. This was an increase of 2 per cent over the previous year. Possible misconduct existed in more than two-thirds of all failures in that reporting period.²⁸

The expanded director penalty regime now makes directors personally liable for their company’s outstanding pay-as-you-go (PAYG) withholding and superannuation guarantee. This reduces the scope for companies to escape paying employee entitlements for associated liquidated companies, but does not make them liable for other outstanding debts.

25 Also known as ‘boiler-room’ fraud, cold-calling investment fraud refers to the unsolicited contacting of potential investors who are deliberately given fraudulent, false, misleading or deceptive information designed to entice them to buy, sell or retain securities or other investments. This fraud attracts victims with promises of high financial returns and claims of low risk investment strategies.

26 PricewaterhouseCoopers 2012, *Phoenix activity: sizing the problem and matching solutions*, Fair Work Ombudsman, Canberra, June 2012.

27 Australian Securities and Investments Commission 2014, *Annual Report 2013–2014*, ASIC, Sydney.

28 Australian Securities and Investments Commission 2013, *Report 372: Insolvency statistics: external administrators’ reports (July 2012 to June 2013)*, ASIC, Sydney, October 2013, p. 6.

CASE STUDY

FRAUDULENT PHOENIXING ACTIVITY

An earthmoving, garden supplies and property development business based in Perth created fake payment summaries, moved employees between related companies, and failed to remit monies withheld from employees' wages to the ATO. The business owner then deregistered the (non-compliant) companies to reduce the risk of detection by authorities.

The principal company director was sentenced to five years and three months jail for defrauding the Commonwealth of A\$6.7 million in unremitted taxes. He was also bankrupted after an investigation into his personal tax affairs. A number of other people associated with this fraud have also been prosecuted and jailed, including a former tax agent.¹

1 Australian Taxation Office, *The fight against tax crime: fraudulent phoenix activities*, ATO, viewed 15 January 2015, <<https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Fraudulent-phoenix-activities/>>.

The ATO has noted an increase in phoenixing activity to facilitate tax evasion, and law enforcement has seen increasing evidence of organised crime involvement in the type of industries susceptible to phoenixing.

Fraudulent use of trust structures

Despite trusts playing a legitimate role in the protection of assets and estate planning, the exploitation of trust structures, particularly those established in offshore tax havens, has been identified (see the case study on page 27). The exploitation of trust structures is used to conceal the ultimate beneficial ownership of underlying assets, and for large-scale revenue and taxation fraud activities.

Most of the 700,000 trusts now registered in the Australian tax system are discretionary trusts used for a wide variety of legitimate business and investment activities. However, in relation to phoenixing, the ATO has noted an emerging scheme that involves interposing shell companies as trust beneficiaries and then liquidating these companies before trust tax debts are paid.

As trust structures are more expensive and potentially complicated to establish, and have more complex administration and taxation aspects than other types of business structures, there is an enhanced requirement to use professional facilitators.

CASE STUDY

ABUSIVE USE OF TRUST ACTIVITIES

The abusive use of trusts was employed to avoid in excess of A\$50 million in tax in the property development sector over a period of 10 years. It involved the siphoning off of profits from the main entities to trusts and companies controlled by the principal and their siblings, with these profits then remitted offshore.

In some cases, completed properties were transferred below market value to related trusts, before being re-valued to market and fully mortgaged, with the finance raised purportedly committed to a sham offshore property development syndicate. These funds were subsequently represented as having been lost. This had the effect of understating assessable profits, creating insolvency and recovery difficulties, and transferring wealth offshore without tax being paid. The case also involved related straw directors (including offshore nominee directors), and raised doubts about the independence of appointed liquidators.

Professional facilitators

The use of professional facilitators remains a key aspect of the exploitation of business structures by organised crime. Because of the ever-increasing complexity of regulation surrounding financial markets and products, the use of a variety of specialists—some of whom are complicit, and some of whom are unwittingly providing assistance—is required to help criminal groups operate their legitimate and illicit businesses (see the case study on page 28).

The level of professional facilitator involvement can range from concealing illicit funds in a lawyer's trust account, to the use of a network of complicit advisers and specialists establishing complex business structures in numerous offshore jurisdictions.

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.

Organised crime entities can purchase businesses in particular sectors in order to achieve a market share large enough to enable them to manipulate the prices of certain goods and services. This can undermine competitive neutrality, because such entities may have an unfair competitive advantage within industries, which can cause harm to legitimate businesses and to the economy.

CASE STUDY

USE OF BROKERS AND GEOLOGISTS IN INVESTMENT FRAUD

A syndicate identified by the Australian Crime Commission had established a number of 'start-up' companies in the mining and resources sector and had also used coercion to take control of existing companies.

Once the syndicate members had acquired control of significant shareholdings, they undertook aggressive capital-raising and marketing campaigns.

As part of their marketing campaigns, the syndicate employed geologists and company research firms to inflate the potential of mining tenements and exploration projects and release favourable research results with 'buy' recommendations to investors. As the share price inflated, a global network of brokers was employed to sell syndicate members' shareholdings.

Public sector corruption

Introduction

Public sector corruption can be a powerful enabler for organised crime and, as a consequence, organised crime entities continue to target public sector officials who can help them facilitate their criminal enterprises. Although those public officials who can provide immediate assistance to serious and organised crime are targeted specifically, those who may be of use in the future are also targeted more generally.

As noted by Transparency International:

The relationship between organised crime and corruption is a simple one—criminal networks make extensive use of corruption, in its various forms, to carry out criminal activity, avoid investigation and escape prosecution. Conversely, corruption within society propagates and becomes much more entrenched when routinely instrumentalised by organised crime. A type of continuum exists, ranging from co-option of junior level officials, that is, effectively placing them on the crime group's payroll, through infiltration of managerial, senior spheres, to influencing heads of law enforcement agencies and finally ending in the capture of state policies and structures.²⁹

²⁹ Muravska, J, Hughes, W & Pyman, M 2011, *Organised crime, corruption, and the vulnerability of defence and security forces*, Background Paper, Transparency International, London, p. 5.

In particular, the large profits available in Australia's illicit drug markets are a strong motivator for organised crime groups to develop the capability to corrupt in order to facilitate access to those markets. As well, corrupt officials may also assist in the money laundering process—for instance, by providing false identification documents or visas.

As intelligence-driven law enforcement agency and border protection activities become more effective, there is a greater incentive for organised crime to corrupt government officers to gain knowledge and capability to evade them.³⁰ Organised crime would regard corruption of a public official as a 'business cost'.³¹ Accordingly, a focus for Commonwealth law enforcement agencies is to counter potential growth in corruption-enabled border crime, including collusion between officers in different agencies or layers of government.

Corruption can undermine the fundamental trust of the public in government, and in the legitimacy of the instruments of government. Corruption can work insidiously to protect the business of serious and organised crime, and to prevent the identification of criminal behaviour.

Current situation

Australia is perceived as a relatively corruption-free country. Recent declines in Transparency International's Corruption Perceptions Index ranking for Australia—from the seventh least corrupt country in 2012, to the ninth least corrupt country in 2013, and currently to the eleventh least corrupt in 2014³²—perhaps may result from efforts in Australia to deal with major corruption incidents transparently, as much as they may appear to show a deterioration of public sector standards. Australia's overall ranking remains very high and is comparable with the rankings of countries such as the United States, the United Kingdom and Canada.

Australian anti-corruption bodies inform the public's understanding of public sector corruption through investigations and generate important intelligence and insights about corruption risks and systems vulnerabilities. However, anti-corruption agencies have noted a concern that, as the sophistication of organised crime increases, corrupt conduct is likely to become less susceptible to discovery than was previously the case.³³

Two separate streams of vulnerability to corruption by organised crime are becoming apparent to law enforcement and anti-corruption agencies in Australia. The first is the historically identified risk of the corruption of public sector officials whose seniority or role/function puts them in a position in which they can facilitate or protect criminal activities. In some instances, organised crime groups may be more likely to target vulnerable persons in lower levels in the public sector, where their positions offer access to privileged information that could assist organised crime activities. The second is an emerging generational risk posed by younger new recruits. Though the first of these vulnerabilities is well known, an understanding of the second has only recently begun to be developed.

30 Australian Commission for Law Enforcement Integrity 2013, *Annual Report of the Integrity Commissioner 2012–13*, ACLEI, Canberra, p. 73.

31 Australian Commission for Law Enforcement Integrity 2014, *Annual Report of the Integrity Commissioner 2013–14*, ACLEI, Canberra, p. 93.

32 Transparency International Australia assesses that the decline may be attributed to the prosecution of Security and Note Printing Australia executives, and the findings of the Independent Commission Against Corruption (ICAC) in relation to Eddie Obeid and the corruption in the New South Wales Government at the time.

33 Australian Commission for Law Enforcement Integrity 2013, *Annual Report of the Integrity Commissioner 2012–13*, ACLEI, Canberra, p. 5.

Social networking, the sharing of personal information on social media, and casual attitudes and the apparent growing tolerance of the general public toward ‘recreational’ or ‘private’ illicit drug-taking have been identified as having the potential to significantly increase the risk of corruption of younger public sector employees by bringing them into contact with organised crime groups.³⁴

The Australian Commission for Law Enforcement Integrity (ACLEI) has observed that long-term friendships between public officials and those involved in criminal activity can lead to corruption. In one investigation, ACLEI noted that a network ‘shared some common demographics, including school links, age and community ties. These same links and sources of obligation extended to friends who were active members in organised crime groups, including outlaw motorcycle gangs.’³⁵ ACLEI found that this common background allowed the corrupt group to expand with a level of confidence.

ACLEI has also observed an apparent willingness by public sector employees found to have indulged in illicit drug use—particularly cocaine—to construct a personal outlook that artificially demarcates their private lives (socialising with other drug users and drug dealers) from their professional responsibilities (interdicting drugs and taking enforcement action against those involved).³⁶ Importantly, at least some of these employees appear to see nothing wrong with living what amounts to a double life. ACLEI investigations have also suggested that some employees who engage in illicit drug use have responded to the introduction of mandatory random drug-testing schemes by adopting measures designed to defeat drug tests.³⁷

Inappropriate relationships are consistently identified in corruption investigations. These relationships can develop opportunistically or through deliberate targeting on the part of organised crime. Corrupt public sector officials have been observed to target their colleagues by building trust, social obligation and complicity over time. A network increases the corrupt officer’s capability to engage in corrupt conduct, while increasing the opportunity for concealment. Corrupt networks of this type are of significant value to the business model of organised crime groups.

ACLEI has noted that the resignation or removal of a public official from the workplace does not always put a stop to the influence that former officials are able to exert over employees who remain in the workplace, and who may continue to service the needs of organised crime entities.³⁸

34 Australian Commission for Law Enforcement Integrity 2013, *Annual Report of the Integrity Commissioner 2012–13*, ACLEI, Canberra, p. 73.

35 Australian Commission for Law Enforcement Integrity 2013, *Operation Heritage—a joint investigation of alleged corrupt conduct among officers of the Australian Customs and Border Protection Service at Sydney International Airport (Interim Report)*, Investigation Report 02-2013, viewed 13 January 2015, <<http://www.aclei.gov.au/Documents/Reports%20and%20speeches/Report022013-OperationHeritageinterimreport.pdf>>.

36 Australian Commission for Law Enforcement Integrity 2013, *Annual Report of the Integrity Commissioner 2012–13*, ACLEI, Canberra, p. 94.

37 Australian Commission for Law Enforcement Integrity 2014, *Operation Myrrh—an investigation into “private” illicit drug use by certain Australian Customs and Border Protection Service officers*, Investigation Report 01-2014, viewed 3 March 2015, <<http://www.aclei.gov.au/Documents/Reports%20and%20speeches/Report012014AninvestigationintoprivateillicitdrugusebycertainAustralianCustomsandBorderProtectionServiceofficers.pdf>>.

38 Australian Commission for Law Enforcement Integrity 2013, *Annual Report of the Integrity Commissioner 2012–13*, ACLEI, Canberra, p. 95.



CASE STUDY

FOREIGN BRIBERY

An Australian Federal Police (AFP) investigation into allegations that employees of an Australia-based construction company had paid bribes to government officials in Iraq has led to charges being laid against three men for conspiracy to bribe a foreign public official. Police will allege that almost A\$1 million was transferred overseas for payment of these bribes. One of these men has also been charged with a money laundering offence.¹

¹ Australian Federal Police 2015, 'Man arrested for foreign bribery', media release, 20 February 2015, viewed 26 February 2015, <<http://www.afp.gov.au/media-centre/news/afp/2015/february/media-release-man-arrested-for-foreign-bribery>>.

Self-initiated corruption by individual public sector officials also occurs. Positions of power and authority are exploited for personal financial gain and, at times, government officials will actively engage others in the private and public sector to facilitate their corrupt activities. Although this kind of self-initiated corruption does not involve or is not necessarily influenced by organised crime, it still contributes to undermining confidence in the integrity of public sector services and opens these corrupt individuals to being compromised by organised crime.

A broader threat to Australian public sector integrity is posed by acts of foreign bribery. Australia-based corporate bodies operating offshore and bribing foreign officials may be more likely or willing than other corporate bodies to attempt to engage in this type of activity in Australia (see the case study above).

In addition, organised crime and overseas-based companies may see corrupt activity undertaken by Australian businesses offshore as a sign that corruption of officials is considered an appropriate business strategy in Australia, leading to an increase in attempts to corrupt Australian public sector officials based overseas and domestically.

The increased awareness of foreign bribery issues led the AFP to establish an internal Foreign Bribery Panel of Experts in 2012. In early 2013, the AFP established the Fraud and Anti-Corruption Centre to focus on foreign bribery offences and, in May 2013, it joined an International Foreign Bribery Taskforce. The purpose of the taskforce is to enable countries to work collaboratively to strengthen investigations into foreign bribery claims.

The United Nations Office on Drugs and Crime notes that there is a broad consensus among academics, practitioners and politicians that corruption is one of the main obstacles to peace, stability, sustainable development, democracy and human rights globally.

Violence

Introduction

Violence is a key enabler of organised crime-related activities such as extortion, intimidation and crimes against the person. Violence is used by organised crime to gain or retain control of 'turf', to ensure an ongoing stake in illicit markets, as punishment or retaliation for slights or misdeeds, and to collect debts or to send a warning. Violence may also be offered as a contracted and paid service to other crime groups. In some instances, individual group members are permitted to exploit the group's reputation for violence for their own personal profit or gain.

Serious and organised crime groups' use of violence puts lives at risk and, in those instances in which organised crime-related violence is played out in public, violates community safety and diminishes public confidence in law enforcement and governments. The potential harm to the public from violence related to organised crime will increase as organised crime groups become more habituated to committing acts of violence in public spaces.

There is considerable pressure on governments and law enforcement to combat the use of violence by organised crime, with some jurisdictions recently introducing legislation aimed at reducing violence and increasing penalties for violent offences.

Current situation

Violent incidents involving serious and organised crime reported in the media are frequently 'street crime' or opportunistic crime, such as alcohol-related incidents and individually targeted violence. However, in recent years there has been an escalation in outlaw motorcycle gang (OMCG)-driven violence, particularly in the public domain, between rival gangs and, at times, between members of the same OMCG. Often, this violence can put members of the public at risk as well (see the case study on page 33).

Disputes between rival OMCG clubs almost always act as a catalyst for subsequent violent events of retaliation and retribution.

Notably, OMCGs have been reported to recruit new members and associates who have specialist capabilities that can be used in committing violent crime. For example, ex-army personnel with specialist expertise in the use of explosives and weaponry may be actively targeted for recruitment.

Extortion rackets have also been a well-recorded criminal business of organised crime groups, particularly of some OMCG members. Physical violence, intimidation and harassment are synonymous with extortion activities, and may continue to affect victims even after the extorted debt is settled.

CASE STUDY

OMCG VIOLENCE

In April 2012, an OMCG member was responsible for a public shooting at a shopping centre on the Gold Coast, with a rival OMCG member as the target. The rival OMCG member and an innocent bystander in the shopping centre were shot and wounded. The lawyer for the OMCG member argued that the firearm was used in self-defence because the rival OMCG member was wielding a knife.¹ In November 2014, the OMCG member was convicted of attempted murder and unlawful wounding as a result of this incident.

In September 2013, a large public brawl occurred between members and associates of two rival OMCGs at a Gold Coast restaurant. Other diners at the restaurant moved quickly to escape the violence. Following the arrests resulting from the incident, a large group of OMCG members gathered outside the police station where arrested members were being held, as a reported demonstration of intimidation against police.² Forty-three people were charged with 52 offences as a result of the brawl.

In October 2013, another violent brawl occurred between rival OMCGs at a café on the Gold Coast. Members of the public were also present at the time of this incident. It was reported that no one was injured as a result of this incident.

1 'Robina shooter and Mongols bikie Mark James Graham gets 12 years for attempted murder and unlawful wounding', *Gold Coast Bulletin*, 3 November 2014, viewed 20 January 2015, <<http://www.goldcoastbulletin.com.au/news/crime-court/robina-shooter-and-mongols-bikie-mark-james-graham-gets-12-years-for-attempted-murder-and-unlawful-wounding/story-fnje8bkv-1227110457871>>.

2 Ravn, M, Westthorp, T & Laughlin, S 2013, 'Eighteen bikies arrested after Broadbeach brawl', *Gold Coast Bulletin*, 28 September 2013, viewed 15 January 2015, <<http://www.goldcoastbulletin.com.au/news/crime-court/eighteen-bikies-arrested-after-broadbeach-brawl/story-fnje8bkv-1226774457240>>.

The building industry has experienced the use, and threats, of violence through verbal violence and extortion. It is understood that links between organised crime and some people in the building industry have been used to exert pressure and standover tactics in order to influence the outcome of lucrative building and labour contracts.³⁹

39 Oakes, D 2014, 'CFMEU rocked by claims of corrupt dealing with crime figures in exchange for construction contracts', ABC News, 28 January 2014, viewed 5 February 2015, <<http://www.abc.net.au/news/2014-01-28/union-accused-of-ties-to-crime-figures-kickbacks-for-jobs/5221234>>.

The contracting of organised crime by casino junket operators for debt collection from casino 'high-roller' clients through the use of, or at least the threat of, violence has also been reported overseas.⁴⁰ Organised crime–driven violence in high-density gambling locations such as Macau is reported to have thrived through debt collection pressures on indebted high-rollers. With new Australian casinos reported to be marketing to attract international casino junket tours,⁴¹ it is possible that junket tour operators may seek to employ serious and organised crime as contracted standover debt collectors here in Australia.

40 'Organised crime linked to high roller gamblers: concerns for new Australian casinos', *News.com.au*, 15 September 2014, viewed 15 January 2015, <<http://www.news.com.au/finance/money/organised-crime-linked-to-high-roller-gamblers-concerns-for-new-australian-casinos/story-e6frfmci-1227058972551>>; Nicholls, S 2014, 'Secret Packer casino organised crime agreement should be public, independent arbiter finds', *Sydney Morning Herald*, 22 October 2014, viewed 28 January 2015, <<http://www.smh.com.au/nsw/secret-packer-casino-organised-crime-agreement-should-be-public-independent-arbiter-finds-20141022-119tg9.html>>.

41 Nicholls, S 2014, 'Secret Packer casino organised crime agreement should be public, independent arbiter finds', *Sydney Morning Herald*, 22 October 2014, viewed 28 January 2015, <<http://www.smh.com.au/nsw/secret-packer-casino-organised-crime-agreement-should-be-public-independent-arbiter-finds-20141022-119tg9.html>>.



ILLICIT COMMODITIES

Illicit drug market overview

The Australian illicit drug market remains highly lucrative, with the demand for a wide variety of illicit drugs growing. Poly-drug use remains a feature of the Australian drug market, and serious and organised crime groups capitalise on the demand for multiple drug types by importing, producing or trafficking in several drug types simultaneously.

The Australian illicit drug market is best seen as a component of a global market. The Internet and 'darknets' have enabled the rapid expansion of the global drug market, and users can access both drugs, and information about new drugs becoming available, online from anywhere in the world. This has meant that trends in drug use observed in Europe, Canada and the United States—those markets most similar to the Australian market—which once would have taken some time to flow on to the Australian market, are now very quickly replicated in Australia.

Although cannabis remains the most commonly used illicit drug in Australia, with organised crime playing a fundamental role in its large-scale cultivation and distribution, the methylamphetamine market poses the highest risk to Australia, and serious and organised crime groups are entrenched in the market.

The Australian methylamphetamine market has traditionally been supplied by domestically produced product. However, large-scale importations of methylamphetamine, particularly crystalline methylamphetamine, as well as precursor chemicals, are also being detected at the border. This is evidence of an increase in the involvement of transnational organised crime groups in the market, in an effort to capitalise on the profits to be made from the sale of methylamphetamine to a large and expanding market. Users of methylamphetamine are at an increased risk of health-related harms, and the drug can cause violence and aggression, placing those around them at risk of harm as well.

Both the global and the Australian 3,4-methylenedioxymethamphetamine (MDMA, or 'ecstasy') markets continue to regenerate after a period of well-documented shortage. The seizure in November 2014 of almost 2 tonnes of MDMA imported into Australia from Europe is a further indicator of the return of large-scale MDMA manufacture in Europe, as well as the continued recovery of the Australian MDMA market.

Other 'traditional' illicit drugs, such as cocaine, heroin and cannabis, still feature in the Australian market; however, newer substances designed to mimic the effect of traditional illicit drugs—referred to in this report as drug analogues and new psychoactive substances (DANPS)—continue to gain traction. The rapid development of the DANPS market is unprecedented in global illicit drug markets, with 348 substances having been officially reported to the United Nations Office on Drugs and Crime by the end of 2013. Often incorrectly marketed as 'legal' and 'safe' alternatives to illicit drugs, DANPS have been linked to the deaths of several Australian users in recent years.

Organised Crime in Australia 2015 is not intended to provide a comprehensive picture of the Australian illicit drug markets. Detailed overviews of each of the Australian illicit drug markets can be found in the Australian Crime Commission's *Illicit Drug Data Report 2013–14*.

Methylamphetamine

The United Nations Office on Drugs and Crime estimates that amphetamine-type stimulants (ATS), of which methylamphetamine is one, are the second most commonly used illicit drug globally.⁴² In the 2013 National Drug Strategy Household Survey, 'meth/amphetamines'⁴³ were reported as the third most commonly used drug, behind cannabis and 3,4-methylenedioxymethamphetamine (MDMA).⁴⁴ However, innovative research methodologies, such as the analysis of wastewater (sewage), are likely to indicate a much wider use of methylamphetamine in the community. The Australian Crime Commission has assessed the methylamphetamine market as the highest risk drug market in Australia for several years.

In Australia, methylamphetamine has been observed in powder ('speed'), base and crystalline ('ice') forms. Ice use appears to be growing, and many users see ice as the most desirable form of methylamphetamine. This is partly because it is incorrectly perceived to be a purer form of the drug, and partly because it can be smoked rather than requiring intravenous injection. This method of administration may appeal to those users who do not consider themselves to be drug users, and may be a contributor to the expansion of the market. The onset of the effects of ice occur more quickly through smoking, and ice users may be more likely to demonstrate antisocial behaviours, such as violence, than users of other drugs.

⁴² United Nations Office on Drugs and Crime 2014, *World Drug Report 2014*, UNODC, Vienna.

⁴³ Includes both methylamphetamine and amphetamine.

⁴⁴ Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

In a 2014 survey of injecting drug users, 70 per cent of the sample reported that they had used any form of methylamphetamine in the previous six months.⁴⁵ This was the second most commonly reported illicit drug used behind cannabis.⁴⁶ Although reported use of powder and base was stable, there was a significant increase in reported use of ice, up from 55 per cent to 61 per cent of the sample.⁴⁷ The use of ice has been an increasing trend in the annual survey since 2009, when an all-time low of 37 per cent was reported.⁴⁸

The Australian methylamphetamine market has traditionally been supplied by domestically produced methylamphetamine. In recent years, however, there has been a significant increase in the number of detections of ice at the Australian border (see Table 1). Two of the detections alone accounted for 386 kilograms of ice—203 kilograms concealed in an importation of truck tyres detected in September 2013,⁴⁹ and 183 kilograms detected in a consignment of sea kayaks in February 2014.⁵⁰ Furthermore, in November 2014, six men were arrested for the attempted importation of more than 800 kilograms of ice and almost 2 tonnes of MDMA (for further information on this detection, refer to the case study on page 46).

Table 1: Number and weight of ATS and ice detections at the Australian border, 2011–12 to 2013–14⁵¹

	Detections (number)			Weight (kg) ^a		
	2011–12	2012–13	2013–14	2011–12	2012–13	2013–14
Ice	171	1,084	1,379	160.20	1,446.24	1,435.36
Other ATS ^b	907	915	988	187.39	692.30	376.98

a. Weight shown in the above table is an estimate. Weight is calculated using 0.29 grams per tablet where a weight was not available. Some small-quantity shipments of ATS do not have a weight recorded.

b. Includes amphetamines and methylamphetamines in liquid, capsule, paste, powder or tablet form. Figures do not include MDMA or crystalline methylamphetamine (ice).

45 Stafford, J & Burns, L 2014, *Key findings from the 2014 IDRS: a survey of people who inject drugs*, Illicit Drug Reporting System Drug Trends Bulletin, October 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

46 *ibid.*

47 *ibid.*

48 *ibid.*

49 Australian Customs and Border Protection Service 2013, 'Three arrested for importing more than 200kg of methamphetamine in truck tyres', media release, 11 October 2013, viewed 12 February 2015, <<http://newsroom.customs.gov.au/channels/Drugs-and-steroids/releases/three-arrested-for-importing-more-than-200kg-of-methamphetamine-in-truck-tyres>>.

50 Australian Customs and Border Protection Service 2014, 'Drugs worth \$180 million found in kayaks, five people arrested', media release, 12 February 2014, viewed 12 February 2015, <<http://newsroom.customs.gov.au/channels/Drugs-and-steroids/releases/c6b6d870-0338-43df-8add-bfb012aaf939>>.

51 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

This increase in border detections does not appear to have coincided with a decrease in domestic production, as there are still significant precursor chemical and clandestine laboratory detections occurring. For example, 10 people were arrested and 1.9 tonnes of a mixture of vanilla powder and the methylamphetamine precursor pseudoephedrine were seized during an 18-month joint agency investigation that concluded in October 2013.⁵² It is alleged three of those arrested were responsible for distributing the pseudoephedrine–vanilla mix to multiple criminal syndicates within Australia, who would then use it to make methylamphetamine in clandestine laboratories.⁵³ The large increase in border detections, coupled with the ongoing domestic production, suggests that transnational organised crime groups have recognised the strong Australian demand for methylamphetamine and have moved into this lucrative market.

There is significant organised crime involvement in the importation, manufacture and supply of methylamphetamine in Australia. Many of these groups are involved in a range of other activities in addition to methylamphetamine (see the case study on page 39). More than 60 per cent of entities on the National Criminal Target List⁵⁴ are involved in the methylamphetamine and/or precursor markets, and of these more than 80 per cent are also involved in other drug markets. Because there are a number of routes of synthesis requiring a range of precursor chemicals, groups involved in methylamphetamine production can adapt quickly to changes in precursor availability or regulatory controls.

Methylamphetamine is highly addictive and users, particularly the users of crystal methylamphetamine, are at increased risk of a range of health-related harms—most notably increased risk of psychosis and other mental illness. Other harms include headaches, anxiety, paranoia, vision problems, hallucinations, tremors and stroke. Long-term use can result in memory loss, aggression and increased risk of heart failure and stroke.

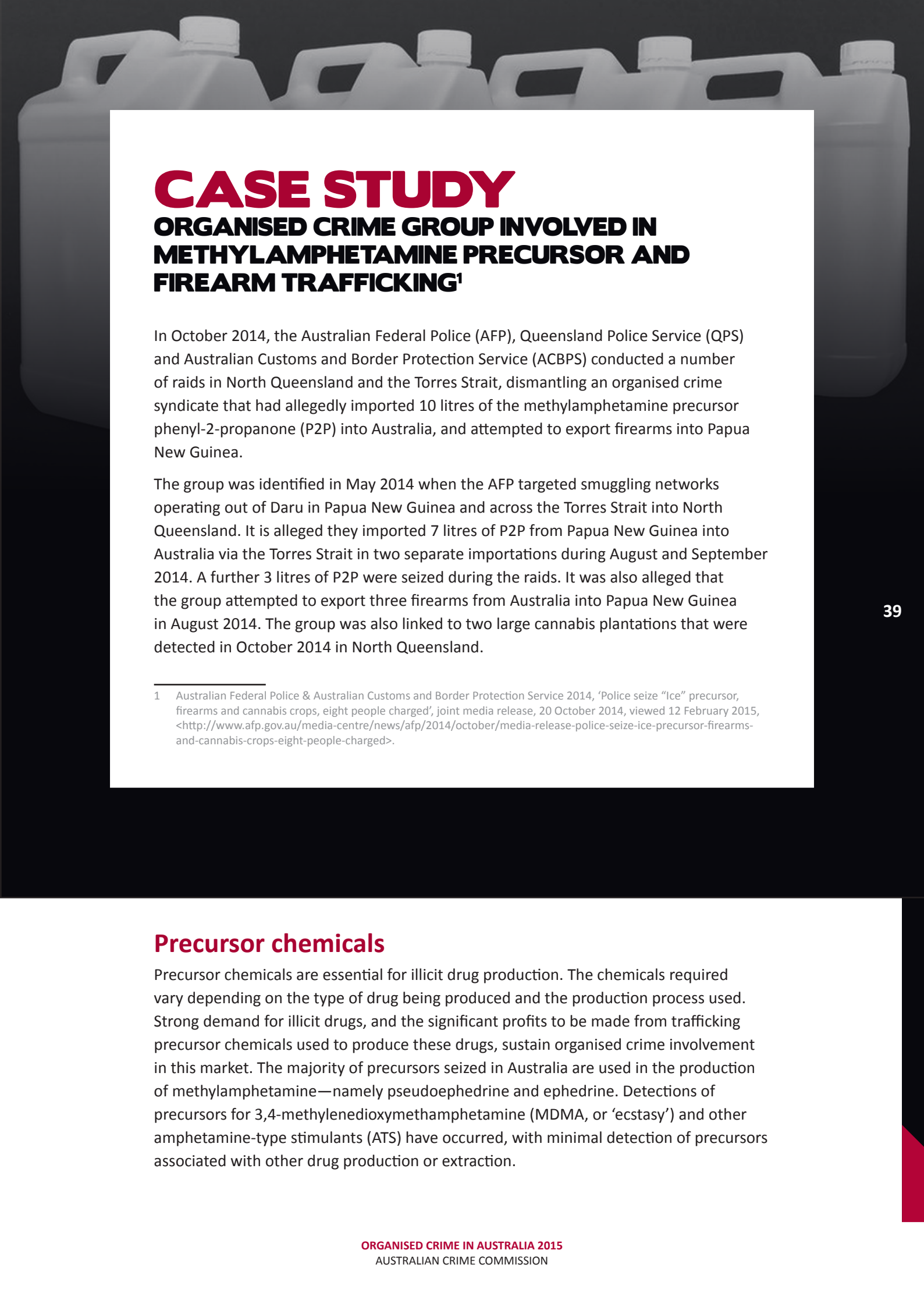
Users and manufacturers are particularly vulnerable to a range of hazards associated with the clandestine manufacture of illicit drugs. Children present in the homes of methylamphetamine users or manufacturers are particularly at risk of ingesting associated chemicals, with one study finding forensic evidence that such children who had experienced ‘low-level’ environmental exposure to methylamphetamine and its manufacture had metabolised as much methylamphetamine as adult users.⁵⁵ Methylamphetamine manufacture in clandestine laboratories has resulted in explosions that have severely damaged properties and resulted in serious injuries and death. These labs are often located in residential areas, posing a risk to the surrounding community.

52 Australian Crime Commission, Australian Customs and Border Protection Service, Australian Federal Police & Victoria Police 2013, ‘International drug syndicate disrupted following joint taskforce investigation’, joint media release, 21 October 2013, viewed 12 February 2015, <<https://www.crimecommission.gov.au/media-centre/release/australian-crime-commission-joint-media-release/international-drug-syndicate>>.

53 *ibid.*

54 The National Criminal Target List is a national listing of currently active and nationally significant organised criminal groups operating in Australia, and is contributed to by Commonwealth, state and territory law enforcement agencies. The total number of entities listed is classified.

55 Bassindale, T 2012, ‘Quantitative analysis of methamphetamine in hair of children removed from clandestine laboratories—evidence of passive exposure?’, *Forensic Science International*, vol. 219, no. 1, pp. 179–82.



CASE STUDY

ORGANISED CRIME GROUP INVOLVED IN METHYLAMPHETAMINE PRECURSOR AND FIREARM TRAFFICKING¹

In October 2014, the Australian Federal Police (AFP), Queensland Police Service (QPS) and Australian Customs and Border Protection Service (ACBPS) conducted a number of raids in North Queensland and the Torres Strait, dismantling an organised crime syndicate that had allegedly imported 10 litres of the methylamphetamine precursor phenyl-2-propanone (P2P) into Australia, and attempted to export firearms into Papua New Guinea.

The group was identified in May 2014 when the AFP targeted smuggling networks operating out of Daru in Papua New Guinea and across the Torres Strait into North Queensland. It is alleged they imported 7 litres of P2P from Papua New Guinea into Australia via the Torres Strait in two separate importations during August and September 2014. A further 3 litres of P2P were seized during the raids. It was also alleged that the group attempted to export three firearms from Australia into Papua New Guinea in August 2014. The group was also linked to two large cannabis plantations that were detected in October 2014 in North Queensland.

¹ Australian Federal Police & Australian Customs and Border Protection Service 2014, 'Police seize "Ice" precursor, firearms and cannabis crops, eight people charged', joint media release, 20 October 2014, viewed 12 February 2015, <<http://www.afp.gov.au/media-centre/news/afp/2014/october/media-release-police-seize-ice-precursor-firearms-and-cannabis-crops-eight-people-charged>>.

Precursor chemicals

Precursor chemicals are essential for illicit drug production. The chemicals required vary depending on the type of drug being produced and the production process used. Strong demand for illicit drugs, and the significant profits to be made from trafficking precursor chemicals used to produce these drugs, sustain organised crime involvement in this market. The majority of precursors seized in Australia are used in the production of methylamphetamine—namely pseudoephedrine and ephedrine. Detections of precursors for 3,4-methylenedioxymethamphetamine (MDMA, or 'ecstasy') and other amphetamine-type stimulants (ATS) have occurred, with minimal detection of precursors associated with other drug production or extraction.

Large amounts of precursor chemicals continue to be seized at the border (see the case study on page 41), with China and India, in particular, being identified as primary source countries. Precursor chemicals are also diverted domestically from the legitimate chemical supply chain. An emerging importation methodology is precursor masking, in which the chemical structure of the substance is altered to avoid detection at the border.

In 2013–14, the Australian Customs and Border Protection Service detected 1,170 attempted precursor importations, 88 per cent of which were precursors for the production of amphetamine-type stimulants.⁵⁶ Although the numbers are relatively low, there has been an increase in detections of precursors for gamma-hydroxybutyrate (GHB), increasing from 47 detections in 2011–12 to 104 detections in 2013–14.⁵⁷

Cocaine

The majority of the world's coca cultivation occurs in the South American countries of Colombia,⁵⁸ Bolivia⁵⁹ and Peru,⁶⁰ with global coca cultivation fluctuating in recent years. Despite a 17.5 per cent decrease between 2012 and 2013, Peru has remained the largest global coca cultivator (ahead of Colombia) for the second year in a row.

In line with these figures, of the seizures analysed, most cocaine seized at the Australian border originates from coca grown in Colombia or Peru. Small amounts of cocaine from Bolivia, or of mixed origin, have also been detected.⁶¹

The Australian cocaine market varies across jurisdictions, with the majority of cocaine use occurring in New South Wales and Victoria.⁶² However, it remains difficult to obtain an accurate estimate of the prevalence of cocaine use among the general population because of the 'hidden' nature of much of the user base (as cocaine users are less likely to come to the attention of authorities), and less cocaine appears to be used in Australia compared with other illicit stimulants. Innovative research strategies, such as the analysis of wastewater (sewage), have been used in Europe to monitor illicit drug use trends and compare drug use in different cities, or across different time periods.⁶³ These types of strategies have also been used in some parts of Australia, albeit to a lesser extent, and may provide a more accurate picture of the prevalence of cocaine use, as neither cocaine nor its metabolite is produced by consumption of other drugs or environmental sources.⁶⁴

56 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

57 *ibid.*

58 United Nations Office on Drugs and Crime 2014, *Colombia coca cultivation survey 2013*, United Nations, Colombia.

59 United Nations Office on Drugs and Crime 2014, *Estado Plurinacional de Bolivia monitoreo de cultivo de coca 2013*, United Nations, Bolivia.

60 United Nations Office on Drugs and Crime 2014, *Monitoreo de cultivos de coca 2013*, United Nations, Peru.

61 Australian Crime Commission 2014, *Illicit Drug Data Report 2012–13*, ACC, Canberra.

62 Roxburgh, A, Ritter, A, Slade, T & Burns, L 2013, *Trends in drug use and related harms in Australia, 2001 to 2013*, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

63 Gerrity, D, Trenhom, RA & Snyder, SA 2011, 'Temporal variability of pharmaceuticals and illicit drugs in wastewater and the effects of a major sporting event', *Water Research*, vol. 45, no. 17 (November 2011), pp. 5399–411.

64 Prichard, J, Lai, FY, Kirkbride, P, Bruno, R, Ort, C, Carter, S, Hall, W, Gartner, C, Thai, PK & Mueller, JF 2012, *Measuring drug use patterns in Queensland through wastewater analysis*, Trends and Issues in Crime and Criminal Justice no. 442, Australian Institute of Criminology, Canberra.

CASE STUDY

ATTEMPTED IMPORTATION OF 50 LITRES OF PSEUDOEPHEDRINE¹

In June 2013, the Australian Crime Commission disseminated intelligence to the Australian Federal Police relating to a possible importation of precursor chemicals through a chemical supply business, alleged to have been set up solely to mask the importation of the restricted precursor.

In August 2014, Customs officers inspected a consignment of chemicals ordered by the company. During this inspection, 10 five-litre drums containing pseudoephedrine suspended in liquid form were detected. Based on the purity, the precursor seized could have been used to produce methylamphetamine worth almost A\$10 million.

The joint-agency investigation continued until late October 2014, when search warrants were carried out in Adelaide and Sydney. Two men were arrested and charged with the importation.

¹ Australian Customs and Border Protection Service, Australian Crime Commission, Australian Federal Police & South Australia Police 2014, 'Joint operation sees two men charged with importing precursor chemicals', joint media release, 22 October 2014, viewed 15 January 2015, <<http://www.afp.gov.au/media-centre/news/afp/2014/october/joint-operation-sees-two-men-charged-with-importing-precursor-chemicals.aspx>>.

Over the last 20 years, there has been a steady increase in the number of respondents to the 2013 National Drug Strategy Household Survey reporting they had ever used cocaine, up from 2.5 per cent in 1993 to 8.1 per cent in 2013.⁶⁵ The proportion of respondents reporting cocaine use in the 12 months prior to interview is much smaller, but still the equal highest on record, at just 2.1 per cent of the Australian population.

Analysis of annual drug user survey results between 2001 and 2013 shows fluctuations in patterns of reported recent cocaine use at the time of the survey. Among injecting drug users, there has been a significant decline in recent cocaine use, as well as a decrease in the proportion reporting cocaine use weekly or more often.

⁶⁵ Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

However, during the same period, recent cocaine use among regular ecstasy and related drug users increased from 23 per cent in 2003 to a peak of 48 per cent in 2010, then declining to 30 per cent in 2013.⁶⁶ In 2014, this proportion increased significantly to 44 per cent, with all states except Western Australia reporting an increase.⁶⁷ It is unclear why there has been a difference in cocaine use between these two groups over time, but factors such as the different demographics of the samples, differing levels of income and/or drug preference, or reduced availability within the injecting drug user market are likely contributors.

There is significant organised crime involvement in the Australian cocaine market, with a diverse range of organised crime groups being identified in the importation and trafficking of cocaine. The Australian Customs and Border Protection Service made 1,512 detections of cocaine, weighing 245.57 kilograms, in 2013–14.⁶⁸ This was a reduction from the 2,003 detections weighing 399.69 kilograms in 2012–13.⁶⁹

Heroin

The majority of the world's illicit opium poppy cultivation occurs in South West and South East Asia and Latin America. The United Nations Office on Drugs and Crime estimates that, globally, in 2013 there were more than 296,000 hectares of opium under cultivation—the highest level in more than 10 years.⁷⁰ Afghanistan is the leading cultivator and producer of opium globally. Between 2013 and 2014, opium poppy cultivation in Afghanistan increased by 7 per cent and the estimated potential opium production in Afghanistan increased 17 per cent, from 5,500 tonnes to 6,400 tonnes. Typically, opium is converted into heroin in, or close to, the countries where the opium poppy is cultivated, although poppy eradication and opium and morphine seizures are reported in a wide range of countries other than the main opium-producing countries.

Historically, the Australian heroin market has been supplied with heroin originating from South East Asia. However, South West Asian heroin has been detected in varying proportions over the last decade. In 2011, South West Asian heroin accounted for 51 per cent of the number of border detections analysed, before dropping back to 26 per cent in 2012.⁷¹

There is significant organised crime involvement in the importation and distribution of heroin in Australia. There has been a general downward trend in the number of heroin detections at the Australian border since 2006–07, while the weight of those detections has fluctuated. In 2013–14, the Australian Customs and Border Protection Service made 180 detections of heroin, weighing 118.89 kilograms.⁷² This was a reduction from the 237 detections weighing 513.82 kilograms in the previous year.⁷³

66 Roxburgh, A, Ritter, A, Slade, T & Burns, L 2013, *Trends in drug use and related harms in Australia, 2001 to 2013*, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

67 Sindich, N & Burns, L 2014, *An overview of the 2014 Ecstasy and Related Drugs Reporting System*, EDRS Drug Trends Bulletin, October 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

68 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

69 *ibid.*

70 United Nations Office on Drugs and Crime 2014, *World Drug Report 2014*, United Nations, Vienna.

71 Australian Crime Commission 2014, *Illicit Drug Data Report 2012–13*, ACC, Canberra.

72 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

73 *ibid.*

Determining the level of heroin use in the general population is difficult because users are often not captured in general population surveys. In the 2013 National Drug Strategy Household Survey, only 0.1 per cent of Australians reported heroin use in the preceding year.⁷⁴ This proportion has been steadily decreasing since 1998.

Domestic market indicators suggest that the Australian heroin market has remained stable and consists of an entrenched and ageing user population. Analysis of the 2014 Illicit Drug Reporting System data indicated that, among injecting drug users, heroin was the most commonly reported drug of choice and the drug injected most often in the month before the survey.⁷⁵ Further analysis indicated that those who had recently used heroin were significantly more likely than those who had not recently used heroin to have begun injecting drugs earlier in life, to have a longer injecting drug use history, to be currently in drug treatment, to have a prison history, to have injected at least daily in the previous month, to have very high psychological distress levels, and to have riskier injecting practices.⁷⁶

Drug analogues and new psychoactive substances

Drug analogues and new psychoactive substances (DANPS) are synthetically created substances that have a similar chemical structure to an illicit drug, or that mimic the effects of illicit drugs. Often (incorrectly) referred to as 'legal' alternatives to proscribed substances, DANPS are also known as novel substances, novel psychotropic substances, emerging psychoactive substances, analogues, mimetics, legal highs, new synthetics, synthetics, herbal highs or designer drugs,⁷⁷ and they comprise a range of substances, including stimulants, hallucinogens, anaesthetics and cannabimimetics (also known as synthetic cannabinoids).

There continues to be an increasing range of DANPS manufactured and distributed to the market. The number of DANPS on the global market more than doubled between 2009 and 2013, with 348 substances being reported to the United Nations Office on Drugs and Crime by the end of 2013.⁷⁸

DANPS have been available in the Australian market since the mid-2000s, but have increased in availability and popularity in recent years. In 2013, the National Drug Strategy Household Survey included the new categories of 'synthetic cannabinoids' and other 'new and emerging psychoactive substances' for the first time. Reported use was relatively low in the general population, with 1.2 per cent of the population reporting synthetic cannabinoid use and 0.4 per cent reporting use of other new and emerging psychoactive substances in the previous 12 months. However, this level of use is similar to that reported for hallucinogens and tranquillisers, and much higher than the reported use of other illicit drugs such as heroin, ketamine and gamma-hydroxybutyrate (GHB).

74 Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

75 McIlwraith, F, Hickey, S & Alati, R 2014, *What's happening with heroin?*, Illicit Drug Reporting System Drug Trends Bulletin, December 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

76 *ibid.*

77 Australian Crime Commission 2014, *Illicit Drug Data Report 2012–13*, ACC, Canberra.

78 United Nations Office on Drugs and Crime 2014, *World Drug Report 2014*, UNODC, Vienna.

Less than 5 per cent of recent synthetic cannabinoid users reported having not used any other illicit drug during the same 12-month period.⁷⁹

Results from the 2014 Ecstasy and Related Drugs Reporting System (EDRS) survey show that recent use of 'new psychoactive substances'⁸⁰ remained stable at 36 per cent of the national sample. For the first time, respondents were asked if they had specifically sought out new psychoactive substances or if they had been offered them by others. Half of the sample (50 per cent) reported specifically seeking out new psychoactive substances, suggesting that these substances are not simply used to supplement illicit drug use, but may also be sought out as alternatives to illicit use of other drugs.⁸¹

There was a significant decrease in EDRS respondents reporting recent use of synthetic cannabinoids between 2013 and 2014 (from 16 per cent to 7 per cent). It is believed that this decline in use is related to users' negative reports about both the high and the comedown after using the substances.⁸²

DANPS are often marketed as 'safe' alternatives to illicit drugs. However, DANPS have been linked to a number of deaths in Australia and overseas. In January 2015, the deaths of two men in Queensland were believed to be linked to the use of synthetic cannabinoids.

Production of DANPS at a commercial level has been detected in Australia, including production by people with no prior history of drug use or supply.⁸³ There is a low level of organised crime involvement in the importation and supply of DANPS to the Australian market. The Internet is also a major facilitator, providing a medium for sales, information sharing and social commentary on substances.

MDMA

The global market for 3,4-methylenedioxymethamphetamine (MDMA, or 'ecstasy') is continuing to resurge after a well-documented period of reduced availability. In August and October 2013, European authorities dismantled the two largest clandestine MDMA laboratories ever detected in Europe. Several tonnes of the precursor safrole and more than 1 tonne of crystal MDMA were seized at the first laboratory,⁸⁴ while 35 tonnes of precursors and other chemicals were seized from the second laboratory.⁸⁵

79 Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

80 The EDRS category of 'new psychoactive substances' does not include synthetic cannabinoids, but does include dimethyltryptamine, which is dealt with in the tryptamines chapter of this document.

81 Sindicich, N & Burns, L 2014, *An overview of the 2014 Ecstasy and Related Drugs Reporting System*, EDRS Drug Trends Bulletin, October 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

82 *ibid.*

83 Crime and Corruption Commission 2015, *New synthetic drugs—deceptive and dangerous*, CCC, Brisbane.

84 Europol 2013, 'Largest ecstasy lab ever found in Europe dismantled', media release, 28 August 2013, viewed 12 December 2014, <<https://www.europol.europa.eu/content/largest-ecstasy-lab-ever-found-europe-dismantled>>.

85 Europol 2013, 'Police discover largest synthetic drugs production site ever found in EU', media release, 23 October 2013, viewed 12 December 2014, <<https://www.europol.europa.eu/content/police-discover-largest-synthetic-drugs-production-site-ever-found-eu>>.

In both instances, the laboratories had been established in rural farming areas in Belgium. The sheer size of the laboratories, a large increase in seizures of precursor chemicals in Europe and a warning in February 2014 about tablets detected in the Netherlands, Belgium, the United Kingdom and Switzerland containing potentially fatal levels of MDMA⁸⁶ are clear indications that MDMA production in Europe has increased significantly.

The Australian MDMA market, as a component of the global MDMA market, is also regenerating. Though the number and weight of MDMA detections at the Australian border fell from 4,139 detections weighing 149.27 kilograms in 2012–13 to 3,247 detections weighing 94.82 kilograms in 2013–14, the 2013–14 figures are nonetheless significantly higher than the 964 detections weighing 11.95 kilograms in 2011–12.⁸⁷ A further indicator of resurgence in the global and domestic MDMA markets is the seizure of almost 2 tonnes of MDMA in New South Wales in November 2014—the second-largest seizure of MDMA in Australian history (see the case study on page 46).

Although the majority of MDMA consumed in Australia is imported, seizures of precursor chemicals domestically and at the border, and detections of clandestine laboratories, indicate some level of domestic production. The annual number of detections of MDMA clandestine laboratories in Australia is low, with just seven being detected in 2012–13 (less than 1 per cent of all clandestine laboratory detections that year).⁸⁸

The 2013 National Drug Strategy Household Survey reported a decrease in the proportion of the population who had used MDMA in the previous 12 months (from 3 per cent in 2010 to 2.5 per cent in 2013), but it is still the second most commonly used drug in Australia.⁸⁹ MDMA is most commonly consumed in tablet form, but in 2014 there was a significant increase in the number of regular users reporting the use of crystal MDMA in the Ecstasy and Related Drugs Reporting System (EDRS) survey.⁹⁰ Crystal MDMA is absorbed into the digestive system at a higher rate than in pill or powder form, and as a result users experience a stronger ‘peak’ effect and longer-lasting after-effects.⁹¹ It is unclear when crystal MDMA was introduced to the Australian market, but its use has been reported in the EDRS since 2012.⁹²

86 Europol and European Monitoring Centre for Drugs and Addiction 2014, ‘Tablets with dangerously high levels of MDMA’, Early Warning Notification 2014/6, viewed 12 December 2014, <https://www.europol.europa.eu/sites/default/files/publications/ewn_high_concentration_mdma_feb_2014_-_public.pdf>.

87 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

88 Australian Crime Commission 2014, *Illicit Drug Data Report 2012–13*, ACC, Canberra.

89 Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

90 Sindicich, N & Burns, L 2014, *An overview of the 2014 Ecstasy and Related Drugs Reporting System*, EDRS Drug Trends Bulletin, October 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

91 Entwistle, G & Burns, L 2014, ‘Crystal MDMA: a unique addition to Australian markets’, National Drug Trends Conference poster presentation, viewed 12 December 2014, <[https://ndarc.med.unsw.edu.au/sites/default/files/newsevents/events/Poster%20\(NSW%20EDRS\)%20-%20Crystal%20MDMA.pdf](https://ndarc.med.unsw.edu.au/sites/default/files/newsevents/events/Poster%20(NSW%20EDRS)%20-%20Crystal%20MDMA.pdf)>.

92 *ibid.*

CASE STUDY

A\$1.5 BILLION SEIZURE OF MDMA AND CRYSTAL METHYLAMPHETAMINE¹

In late November 2014, members of the Joint Organised Crime Group (JOCG)² arrested six men in relation to the seizure of illicit drugs estimated to be worth up to A\$1.5 billion on the street. Almost 2 tonnes of MDMA and more than 800 kilograms of crystal methylamphetamine were hidden inside a mixed container-load of furniture and unmarked boxes shipped to Australia from Germany.

Police conducted a controlled delivery of the consignment to an address in Blacktown in Sydney, where its contents were removed and transported to another location. The six men were arrested when they were found accessing the boxes from the consignment at an address in Smithfield, also in Sydney.

1 Australian Crime Commission, Australian Customs and Border Protection Service, Australian Federal Police, New South Wales Crime Commission & New South Wales Police Force 2014, 'Drugs worth \$1.5 billion seized by Joint Organised Crime Group', joint media release, 29 November 2014, viewed 9 December 2014, <<https://crimecommission.gov.au/media-centre/release/australian-crime-commission-joint-media-release/drugs-worth-15-billion-seized>>.0

2 The JOCG comprises staff from the AFP, the NSW Police Force, the ACBPS, the NSW Crime Commission and the ACC.

Cannabis

Cannabis is cultivated in almost every country of the world, and is the most commonly produced and used illicit drug globally.⁹³ The cannabis market is the largest illicit drug market in Australia, with Australian use reported to be above the global average.⁹⁴ The 2013 National Drug Strategy Household Survey reported that more than one in three Australians had ever used cannabis in their lifetime, and one in 10 had used it in the previous 12 months.⁹⁵

The Australian cannabis market is supplied almost wholly by domestically cultivated cannabis. With the exception of cannabis seeds, oil and resin, it is not profitable or necessary to import cannabis into Australia.

93 United Nations Office on Drugs and Crime 2014, *World Drug Report 2014*, UNODC, Vienna.

94 *ibid.*

95 Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

In 2013–14, the Australian Customs and Border Protection Service made 2,840 detections of cannabis, weighing just 158.07 kilograms.⁹⁶ The majority of the detections were of cannabis seeds.

Organised crime and other low- to medium-level criminal networks are well established in the Australian cannabis market, capitalising on the market's profitability and strength, though the nature and extent of this involvement vary from state to state. There is considerable diversity in the size and sophistication of cannabis cultivation in Australia, from small-scale 'personal use' cultivation through to large, sophisticated, indoor hydroponic 'grow houses' and large outdoor cannabis crops. The cultivation methodology varies depending on the group involved and the location.

Organised Crime in Australia 2013 reported on the then increase in the availability of synthetic cannabinoids, which are often incorrectly marketed as 'legal' alternatives to cannabis. The popularity and availability of these products have continued to grow since then. The use of these products is discussed in the 'Drug analogues and new psychoactive substances' chapter of this report.

Illicit pharmaceuticals

The illicit pharmaceutical market in Australia includes the use of prescription pharmaceuticals in a way that is inconsistent with their intended use or directions, such as intentional misuse or overuse (also referred to as non-medical use), as well as the diversion of pharmaceuticals to the illicit market. Illicit pharmaceuticals may be used in conjunction with, or as an alternative to, illicit drugs. They may also be used to manage the effects of other drugs. A wide range of pharmaceuticals may be misused, including anti-depressants, anti-psychotics and stimulants, but the most commonly misused pharmaceuticals in Australia are opioid analgesics and benzodiazepines.

An international study by INTERPOL in 2014 identified two well-established organised crime groups, as well as outlaw motorcycle gangs (OMCGs), as being involved in pharmaceutical crime,⁹⁷ although this activity was limited in comparison with their involvement in other illicit drug and weapons trafficking.⁹⁸ Aside from these three groups, INTERPOL found that well-established hierarchical groups were not generally involved in pharmaceutical crime, but that it tended to be dominated by:

- highly organised, yet generally informal, international affiliate networks selling medicines through illicit online pharmacies, and
- small groups, not yet well established, of between 3 and 10 members, involved in various aspects of pharmaceutical crime.⁹⁹

⁹⁶ Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

⁹⁷ Pharmaceutical crime was defined as 'the manufacturing and distribution of counterfeit or falsified (spurious/fake/ falsely labelled) pharmaceuticals or medical devices, through licit and illicit supply chains, involving: theft, fraud, diversion, smuggling, illegal trade, money laundering, corruption'.

⁹⁸ INTERPOL 2014, *Pharmaceutical crime and organized criminal groups: an analysis of the involvement of organized criminal groups in pharmaceutical crime since 2008*, INTERPOL Pharmaceutical Crime Sub-Directorate, Lyon.

⁹⁹ *ibid.*

In Europe and North America, organised crime groups, including the Hell's Angels OMCG, have been associated with the manufacture and distribution of counterfeit pharmaceuticals, such as performance and image enhancing drugs.¹⁰⁰ Elsewhere in Europe, organised crime groups have been involved in the robbing of trucks transporting pharmaceutical drugs.¹⁰¹ In Central and South America, there are clear signs of counterfeit production, with finished illicit medicines or raw materials for illicit production exported to other countries in the region.¹⁰²

In Australia, the Pharmaceutical Benefits Scheme subsidises the cost of a broad range of medicine for most medical conditions, ensuring that Australians have affordable access to pharmaceutical medicines, particularly in comparison with some other regions in the world. As a result, there is little demand for potentially counterfeit illicit pharmaceuticals purchased online.

Within Australia, illicit pharmaceuticals can be obtained a number of ways, including by obtaining a legitimate prescription (and then misusing the drugs), by theft or forgery of prescriptions, by purchasing on the illicit market or through the Internet, by diversion from family or friends, or through 'doctor shopping' (visiting multiple doctors to obtain multiple prescriptions).¹⁰³ Because of the relative ease with which pharmaceuticals can be obtained for non-medical use in Australia, there are few opportunities for organised criminal involvement. Although there are organised networks involved in the diversion and distribution of some pharmaceuticals, these tend to be networks of users who are on-selling for profit.

The 2013 National Drug Strategy Household Survey reported a significant increase in the non-medical use of pharmaceuticals, from 4.2 per cent in 2010 to 4.7 per cent in 2013.¹⁰⁴ Only cannabis recorded a higher proportion of recent use in the survey. Recent non-medical use of pharmaceuticals was highest for those aged in their 20s and 30s; however, people aged over 60 were the next highest group to report recent non-medical use.¹⁰⁵ The Australian Crime Commission assesses that the illicit pharmaceuticals market has the potential to increase in threat in the medium term.

Opioid analgesics

Opioid analgesics (or narcotic analgesics) are derived from the opium poppy and act on the central nervous system in a similar manner. They are primarily prescribed for pain management or the treatment of heroin or other opioid addiction. Commonly misused opioid analgesics include codeine, morphine, oxycodone, fentanyl and methadone.

¹⁰⁰ *ibid.*

¹⁰¹ *ibid.*

¹⁰² *ibid.*

¹⁰³ Roxburgh, A, Ritter, A, Slade, T & Burns, L 2013, *Trends in drug use and related harms in Australia, 2001 to 2013*, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

¹⁰⁴ Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

¹⁰⁵ *ibid.*

The misuse of opioid analgesics is relatively low in the general population. The 2013 National Drug Strategy Household Survey found that just 0.2 per cent of the population reported recent non-medical use of methadone or buprenorphine, and 0.4 per cent reported recent use of 'other opiates/opioids'.¹⁰⁶ A larger proportion (3.3 per cent) reported recent non-medical use of painkillers/analgesics, although it should be noted that this category includes both prescription and non-prescription medications, such as ibuprofen and paracetamol.¹⁰⁷

Opioid analgesics may be misused to supplement or as a substitute for heroin use. Results from the annual Illicit Drug Reporting System survey and the annual Australian Needle and Syringe Program Survey¹⁰⁸ indicate that misuse of opioid analgesics tends to be higher in the Northern Territory and Tasmania, where heroin availability is lower than in other jurisdictions,¹⁰⁹ as well as in some Indigenous communities.

Benzodiazepines

Benzodiazepines are minor tranquillisers that are commonly prescribed to relieve insomnia, anxiety and panic attacks. Benzodiazepines may be misused to manage the effects of stimulant drugs (such as methylamphetamine or cocaine), or as a substitute for or to enhance the effects of other depressant drugs.

Although there was a significant increase in the proportion of people reporting they had ever used 'tranquillisers/sleeping pills' for non-medical use in the 2013 National Drug Strategy Household Survey (up from 3.2 per cent in 2010 to 4.5 per cent in 2013), the proportion reporting recent use remained stable at 1.6 per cent (1.5 per cent in 2010).

Performance and image enhancing drugs

In recent years, the performance and image enhancing drugs (PIEDs) market in Australia appears to have grown rapidly, and now consists of users from an increasingly diverse demographic who are using an ever-widening range of substances. Peptides and human growth hormone have gained in popularity among PIEDs users, and are being used in combination with, and in addition to, anabolic steroids. One of the key drivers of the market is a strong youth culture, particularly prevalent among young males, that is focused on a muscular and athletic physical appearance.

The growth in the market appears to have led to an increase in individuals using needle and syringe programs to facilitate their injection of PIEDs. Results from the annual Australian Needle and Syringe Program Survey show a significant increase in respondents reporting PIEDs as the last drug they had injected, from 2 per cent in 2009 to 7 per cent in 2013, with significant increases being reported in Queensland and New South Wales.¹¹⁰

¹⁰⁶ *ibid.*

¹⁰⁷ *ibid.*

¹⁰⁸ Chow, S, Iverson, J & Maher, L 2014, *Drug injection trends among participants in the Australian Needle and Syringe Program Survey, 2009–2013*, Illicit Drug Reporting System Drug Trends Bulletin October supplement 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

¹⁰⁹ Stafford, J & Burns, L 2014, *Australian drug trends 2013—findings from the Illicit Drug Reporting System*, Australian Drug Trends Series no. 109, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

¹¹⁰ Chow, S, Iverson, J & Maher, L 2014, *Drug injection trends among participants in the Australian Needle and Syringe Program Survey, 2009–2013*, Illicit Drug Reporting System Drug Trends Bulletin October supplement 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

The number of PIEDs detections at the Australian border has increased significantly, from fewer than 2,000 in 2008–09 to more than 10,000 in 2012–13.¹¹¹ The number of detections then decreased in 2013–14 to 6,885.¹¹² There is also evidence of the domestic diversion of chemicals used to produce injectable forms of steroids, suggesting possible domestic production of these substances, which may account for some of the decrease in border detections.

Internationally, organised crime groups are heavily involved in the trafficking of PIEDs. Organised crime groups, particularly outlaw motorcycle gangs (OMCGs) and their associates, are involved in the trafficking of PIEDs in the Australian market. PIEDs are also regularly detected at premises where other illicit drugs are located. In January 2015, New South Wales Police and the National Anti-Gangs Squad charged an associate of the Comanchero OMCG in relation to three alleged importations of steroids from China.¹¹³

Anaesthetics

The two most commonly diverted anaesthetics for illicit use in Australia are ketamine hydrochloride (ketamine) and gamma-hydroxybutyrate (GHB), also known as ‘fantasy’. Both substances have well-established, albeit small, niche markets consisting of users primarily based in capital cities along the eastern seaboard.¹¹⁴ There are indications that drug users seeking alternatives to 3,4-methylenedioxymethylamphetamine (MDMA) may have turned to anaesthetics during periods of reduced MDMA availability.

Ketamine

Ketamine is most commonly legitimately used as a medical or veterinary anaesthetic, but is also used illicitly for its sedative and hallucinogenic effects. It is frequently detected as an adulterant in tablets sold as MDMA. The illicit market for ketamine is relatively stable, catering for a small niche group of users. Only 0.3 per cent of the population reported recent ketamine use in the 2013 National Drug Strategy Household Survey.¹¹⁵

Based on responses to the annual Ecstasy and Related Drugs Reporting System survey, ketamine use appears to be concentrated in Victoria and New South Wales. In 2014, 18 per cent of the national sample reported using ketamine in the previous six months.¹¹⁶

In recent years, the proportion of Victorian respondents reporting recent ketamine use has increased significantly, from 20 per cent in 2008 to 63 per cent in 2014.¹¹⁷ Despite the reported increase in recent use in Victoria, ketamine use was infrequent, with a reported median of three days use in the preceding six months (compared with a

111 Australian Crime Commission 2014, *Illicit Drug Data Report 2012–13*, ACC, Canberra.

112 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

113 New South Wales Police Force 2015, ‘Gangs Squad charge man over alleged steroid importation—Strike Force Raptor’, media release, 8 January 2015.

114 Sindich, N & Burns, L 2014, *An overview of the 2014 Ecstasy and Related Drugs Reporting System*, EDRS Drug Trends Bulletin, October 2014, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

115 Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

116 National Drug and Alcohol Research Centre 2014, *Australian drug trends 2014—findings from the EDRS* (Drug Trends Conference handout), NDARC, University of New South Wales, Sydney.

117 *ibid.*

median of two days nationally). It is unclear why the proportion of Victorian respondents reporting recent use has increased at a greater rate than in other jurisdictions; however, because of the small market and infrequency of use, this should not be taken as an indication of market expansion.

Organised crime has not been identified playing a key role in the ketamine market. Ketamine tends to be diverted or imported into the Australian illicit market in relatively small quantities, reflecting personal use or small-scale distribution rather than organised crime involvement.

GHB

GHB is a powerful central nervous system depressant that is readily manufactured from its precursors, gamma-butyrolactone (GBL) and 1,4-butanediol (1,4-BD). GBL and 1,4-BD have legitimate uses as solvents in industrial chemical processes, including the production of polymers. If ingested, both GBL and 1,4-BD metabolise into GHB in the body. The effects of GHB vary greatly depending on the dose, and only a very small increase in dose can lead to overdose.

Like the ketamine market, the Australian GHB market remains stable, supplying a similar small niche group of users. Less than 0.1 per cent of the population reported recent GHB use in the 2013 National Drug Strategy Household Survey.¹¹⁸

As with the ketamine market, results from the Ecstasy and Related Drugs Reporting System survey indicate that GHB use is concentrated in New South Wales and Victoria, but at lower levels. In 2014, just 5 per cent of the national sample reported recent GHB use. Use appeared to be more frequent in Victoria, with a median of 10 days use in the previous six months, compared with a median of two days nationally. However, meaningful conclusions about the significance of this cannot be drawn because of the small size of the market.

Unlike the ketamine market, there are elements of organised crime present in the Australian GHB, GBL and 1,4-BD markets, with some transnational organised crime groups being implicated in suspected importations into Australia. Despite this, the level of sophistication required to operate in this market is quite low, given the ease with which GBL and 1,4-BD can be diverted from the legitimate market.

Tryptamines

Tryptamines are hallucinogenic substances that act on the central nervous system, distorting mood, thought and perception. In Australia the most commonly used tryptamines remain lysergic acid diethylamide (LSD), psilocybin-containing mushrooms (magic mushrooms) and dimethyltryptamine (DMT). Recent years have seen the emergence of a range of hallucinogenic substances that mimic the effect of these substances, but these substances are regarded as drug analogues and new psychoactive substances (DANPS) and are discussed within the DANPS chapter of this report.

¹¹⁸ Australian Institute of Health and Welfare 2014, *National Drug Strategy Household Survey detailed report 2013*, Drug Statistics Series no. 28, Cat. no. PHE 183, AIHW, Canberra.

The tryptamines market, like the anaesthetic market, is a small but complex niche market, making it difficult for law enforcement to obtain an accurate picture of its size and nature. According to the 2013 National Drug Strategy Household Survey, almost one in 10 Australians have used 'hallucinogens' in their lifetime, but only 1.3 per cent reported use in the previous 12 months.¹¹⁹

Results from the 2014 Ecstasy and Related Drugs Reporting System (EDRS) survey show that LSD use is relatively stable, with 41 per cent of the national sample reporting LSD use in the previous six months. Reported use was consistent across most jurisdictions, although the Australian Capital Territory (ACT) reported a significant drop in recent use, from 53 per cent in 2013 to 19 per cent in 2014. Despite this decrease, ACT respondents reported using LSD more frequently than in other jurisdictions, with a median of four days use in the previous six months, compared with two days use nationally.¹²⁰

Although recent use of LSD remained stable, there was a significant decrease in reported recent use of psilocybin-containing mushrooms, from 27 per cent in 2013 to 21 per cent in 2014. Proportions of respondents reporting recent use were similar across all jurisdictions other than the Northern Territory, where it was much lower. Frequency of use was low nationally, with a median of two days use in the previous six months.¹²¹

Recent use of DMT by EDRS respondents remained stable at 14 per cent. The proportion of respondents reporting recent use varied across jurisdictions, from 30 per cent in Victoria to 8 per cent in the Northern Territory. DMT use was infrequent, with a national median of just one day's use in the previous six months.

As with other niche drug markets, tryptamine users are active on social media, contributing to forums and websites to share experiences and source substances. Tryptamine use has long been associated with spiritual and/or religious rituals and regular users have forums dedicated to promoting it. LSD is predominantly self-sourced over the Internet or supplied by friends. Similarly, psilocybin-containing mushrooms are generally obtained for personal use or supplied in close circles, although there has been a recent prosecution for manufacture and supply of a commercial quantity. Given the nature of this market, which frequently includes experimentation with new chemicals for the manufacture of amphetamine-type stimulants, the Internet will continue to have a role in both supplying and promoting tryptamine use.

Intellectual property crime

Intellectual property (IP) is the term used to describe 'the application of the mind to develop something new or original'.¹²² IP crime is a generic term that describes three types of crime markets—counterfeit goods, piracy and the theft of trade secrets.

¹¹⁹ *ibid.*

¹²⁰ National Drug and Alcohol Research Centre 2014, *Australian drug trends 2014—findings from the EDRS* (Drug Trends Conference handout), NDARC, University of New South Wales, Sydney.

¹²¹ *ibid.*

¹²² IP Australia, 'What is IP?', Department of Industry and Science, Canberra, viewed 16 January 2015, <<http://www.ipaustralia.gov.au/understanding-intellectual-property/what-is-ip/>>.

Counterfeit goods

Technology has a key role in facilitating IP crime, making it easier to produce counterfeit goods that appear almost identical to genuine ones. The Internet has made online selling and purchasing of these goods a common practice. One report identifies that:

'it is with the trends of globalisation, the integration of markets and the rise of the Internet economy in recent decades that violations of Intellectual Property Rights (IPR) have become more widespread. Easy access to computers, the Internet and other technological developments facilitate the duplication of designs, labels, logos, packaging and documentation with speed, accuracy and relative anonymity'.¹²³

Counterfeit goods continue to be imported into, and manufactured within, Australia, with the range of goods counterfeited continuing to expand in line with global trends.

Operations by international agencies give some idea of the global size of the market. INTERPOL conducted a one-month operation in parts of Eastern Europe in 2012 that resulted in the seizure of 7.3 million counterfeit goods.¹²⁴ In the same year, the World Customs Organization stated that its members had reported nearly 980 separate brands being counterfeited. The three main product types counterfeited were accessories (15.8 per cent), clothing (14.8 per cent) and pharmaceutical products (10.2 per cent).¹²⁵

In Australia in April 2013, the Commonwealth *Intellectual Property Laws Amendment (Raising the Bar) Act 2012* came into effect. The amendments strengthen processes for seizure of counterfeit goods and allow the Australian Customs and Border Protection Service (ACBPS) to release more information to the rights holder for the genuine goods. This includes details of importers, exporters and others in the supply chain suspected of importing the goods. Such information was not immediately available to rights holders previously and should give increased scope for legal action. Additionally, importers of seized goods now have to make a claim for return of their goods, including providing information to enable the rights owner to locate the importer and initiate legal proceedings for the infringement. This closed a previous loophole that enabled importers of counterfeit or pirated goods to avoid prosecution and still retain the goods.

Since this strengthened legislation was introduced, 99.9 per cent of seized goods suspected to be counterfeit have been forfeited; before these legislative amendments, only 25 per cent of the seized goods suspected to be counterfeit were forfeited.¹²⁶

The ACBPS continues to make large seizures of counterfeit goods at the border (see the case study on page 54). In 2013–14, it made 3,427 separate seizures totalling just less than one million items.¹²⁷ In 2012–13 there were 2,572 seizures totalling 513,814 items, which demonstrates a significant increase in the seizures of counterfeit goods.¹²⁸

123 Hoorens, S, Hunt, P, Malchiodi, A, Liccardo Pacula, R, Kadiyala, S, Rabinovich, L & Irving, B 2012, *Measuring IPR infringements in the internal market: development of a new approach to estimating the impact of infringements on sales*, RAND Corporation, Cambridge, p. vii.

124 Newton, J 2013, 'Introduction: Trafficking in illicit goods—an inclusive INTERPOL programme to combat all types of illicit trade', in *Anti-counterfeiting 2013—a global guide*, INTERPOL, Lyon, p. 22.

125 World Customs Organization 2013, *Illicit Trade Report 2012*, WCO, Brussels, June 2013, p. 87.

126 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

127 Hall, M 2014, 'Nano tracer aims to consign fake goods to the reject pile', *Sydney Morning Herald*, 2 December 2014, viewed 8 December 2014, <<http://www.smh.com.au/it-pro/business-it/nano-tracer-aims-to-consign-fake-goods-to-the-reject-pile-20141201-11xhh5.html>>.

128 Australian Customs and Border Protection Service 2014, *Annual Report 2013–14*, ACBPS, Canberra.

CASE STUDY

LARGE SEIZURE OF COUNTERFEIT GOODS

The World Customs Organization and INTERPOL coordinate an annual international week of action under Operation Pangea, targeting organised crime involvement in the trade in counterfeit and illegal medicines purchased over the Internet. This year, ACBPS officers seized 51 packages containing over 21,000 units of counterfeit or illegal medicines at the Sydney and Melbourne international mail centres, after they had been posted from a range of overseas countries.¹ For the 113 countries participating in this week of action, INTERPOL reported that 434 arrests were made worldwide and suspected counterfeit medicines worth more than US\$36 million were seized.²

-
- 1 Australian Customs and Border Protection Service 2014, 'ACBPS and TGA contribute to worldwide crackdown on counterfeit and illegal medicines', media release, 25 May 2014, viewed 8 December 2014, <newsroom.customs.gov.au/channels/Seizures-cargo-and-mail/releases/acbps-and-tga-contribute-to-worldwide-crackdown-on-counterfeit-and-illegal-medicines>.
 - 2 INTERPOL, 'Operations', viewed 8 December 2014, <<http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea>>.

Most counterfeit goods seized at mail centres are of unknown origin and are suspected of being ordered online. As Internet and online trading can provide greater levels of anonymity, it is not known if those providing the counterfeit goods are organised crime groups or other criminal entities.

Despite the majority of Australian seizures being small and at mail centres, the size of sea cargo seizures, the diversity of goods counterfeited and the sophistication of deception methodologies suggest that organised crime is involved in the importation of counterfeit goods to Australia.

Piracy

Reporting of organised crime involvement in the piracy of film, music, television and computer software continues internationally. Technology continues to make such piracy easier to conduct. For example, an industry study¹²⁹ identified that online film and television piracy is increasing and that 29 per cent of Australian adults aged 18–64 have engaged in online piracy. It was noted that 24 per cent of 12–17-year-olds in Australia admitted using illegal websites to access pirated content, but this peaked with the 18–24 age group, where 54 per cent were engaging in online piracy. Nevertheless, it was also reported that 60 per cent of adults aged 18–64 had never downloaded unauthorised television or movie content online.¹³⁰

It remains likely that organised crime involvement in piracy of these products should decrease as consumers increasingly download them illegally from the Internet without paying. Already some law enforcement agencies have reported that the decrease in the number of detections of pirated copies of music, films, television programs and software has been greater than that observed for other unauthorised goods.

Although the piracy of music, film and television may be becoming less attractive to organised crime, industry reporting suggests that the pirated software market is still profitable. The Business Software Alliance estimates that the commercial value of pirated software increased from US\$58.8 billion in 2010 to US\$62.7 billion in 2013. The Business Software Alliance also calculated that, in 2013, Australia had a software piracy rate of 21 per cent, which is below the global rate of 43 per cent.¹³¹

Trade secrets

Trade secrets provide a distinct business and economic advantage to the holder, and this makes them an attractive target for theft or misappropriation by corporations and governments. Trade secrets are valuable because they give some form of competitive advantage; with this in mind, some businesses do not apply for patents because they know that doing so makes their knowledge or processes public.

Theft of trade secrets is increasing as a concern globally. The real nature and scope of the problem from an Australian perspective is difficult to quantify, as victim companies remain reluctant to report such thefts.

129 Intellectual Property Awareness Foundation 2013, 'New research: the first in-depth study on Australian teens and film and TV piracy—piracy not the 'social norm' in this age group, but almost 1 in 4 teens are active pirates', media release, 30 September 2013, viewed 15 January 2015, <<http://www.ipawareness.com.au/research/2014>>; Bodey, M 2014, 'Australians who download illegally doing it more often', *Australian*, 15 October 2014, viewed 5 March 2015, <<http://www.theaustralian.com.au/business/media/australians-who-download-illegally-doing-it-more-often/story-e6frg996-1227091652438>>.

130 Intellectual Property Awareness Foundation 2014, *2014 research: online behaviour and attitudes of Australians to movie and TV piracy*, viewed 9 December 2014, <<http://www.ipawareness.com.au/research/2014>>.

131 Business Software Alliance 2014, *BSA Global Software Survey—in brief*, The Software Alliance, June 2014, viewed 22 January 2015, <http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_InBrief_a4.pdf>.

In early 2013, the Director-General of the Australian Security Intelligence Organisation (ASIO) was quoted as saying: 'Electronic intelligence gathering is being used against Australia on a massive scale to extract confidential information from governments, the private sector and ordinary individuals. It is used to steal intellectual property, all kinds of defence secrets, weapon designs and commercially advantageous information.'¹³² The media article in which the Director-General of ASIO was quoted also notes the Deputy Director of the then Defence Signals Directorate stating that at least 65 per cent of cyber intrusions have an economic focus.

Although theft of trade secrets is not new, current international economic volatility and the ongoing process of globalisation are likely to be key drivers in the expansion of this crime market. As Australia is an advanced economy increasingly reliant on knowledge-based industries, it is also likely that domestic businesses may be targeted as part of that expansion.

Intellectual property will increase in value as advanced economies transform, with the result that knowledge and ideas will become more tradeable as commodities. This development will see corporations and serious and organised crime groups continue to try to access and misappropriate intellectual property. The harm caused in these new economies could therefore become larger than is presently the case.

The economic costs resulting from IP crime include significant economic consequences through a loss of revenue and the need to invest resources to anticipate and prevent such crime. The loss of confidence in markets and brands has economic implications for producers and investors. International relationships and national security have also been affected by IP-related criminal activity.

Firearm trafficking

For this report, the criminal trafficking of firearms is defined as the movement of illegally owned, modified or manufactured firearms between market suppliers and organised crime. In Australia, there is no single group that dominates the sale and supply of firearms to the illicit market. Both organised crime groups and individual, lower-level criminals drive the demand for illicit firearms. Firearm enthusiasts with no previous criminal involvements can also influence demand by sourcing rare or specialised items from the illicit market because they cannot obtain these items through licit means.

Although there are direct links between firearm trafficking and other serious crimes—for example, the use of illegally obtained firearms in drive-by shootings—this section deals specifically with the issue of trafficking.

Organised crime will continue to acquire and use firearms as an enabler for their area of criminal business, whether it is to protect their interests or to commit acts of violence. Firearms—particularly short-arms—are more likely to be circulated between crime group members so that they can be used for intimidation and threats against rival groups and individuals; to protect their area of criminal operation; and for use in inter-gang or individual conflicts that stem from disputes in other criminal activities such as extortion, outstanding debts and drug repayments. Concealable firearms are also highly sought after by criminals for their portability.

¹³² Loye, C 2013, 'It's global cyber war out there', *Australian Financial Review*, 2 January 2013.

The ‘grey market’ and technical loopholes in legislation continue as historical methods of supplying and diverting firearms to the illicit market. Contemporary methods of supply include theft from licensed individuals and firearm dealers, or the illegal importation of firearms and parts.

The grey market is part of the illicit market and comprises primarily long-arms that were not registered or surrendered in accordance with the 1996 National Firearms Agreement. The grey market is the main source of rifles and shotguns in the illicit market; however, the majority of grey market firearms are believed to be held by ‘non-criminals’. The large pool of long-arms in the grey market, and motivation by criminal entities to obtain firearms, make this a continuing source of supply.

There are also a very small number of individuals who domestically manufacture limited quantities of firearms—in particular, single-shot and sub-machine guns. In Australia, the illicit manufacture of small-calibre single-shot pen guns is a confirmed concern to law enforcement as they are reliable, concealable and effective in firing ammunition.

Recent years have seen the emergence of new threats in the illicit firearms supply to the market. Advances in technology have enabled an online black market for firearms and firearm parts, and ongoing developments in three-dimensional (3D) printing and computer-controlled milling have facilitated the creation of operative firearms.

Online purchasing of illicit firearms remains a threat. Peer-to-peer websites, such as Black Market Revisited and Agora, have enabled the trade in illicit firearms to operate freely, affording anonymity and offering secure online payment systems. Globally, law enforcement has been successful in shutting down darknet websites such as Silk Road; however, other darknet sites are quickly created to fill any void. Before being shut down, Silk Road had closed its site ‘The Armoury’—a website specifically designed to facilitate the trading of firearms, their components and ammunition.

3D printers and milling machines provide those seeking to do so with the capability to successfully create a functional firearm and/or parts. Digital mills are capable of carving firearm frames from aluminium. These frames—with no identifying serial numbers—have the potential to be produced for the illicit market. Currently, 3D-printed firearms may be of low quality, unreliable and expensive to produce; however, recent seizures of 3D-printed firearm parts demonstrate that software and hardware advances and decreased manufacturing costs may make 3D printing of firearms or firearm parts an increasingly viable option in the future.¹³³ Accordingly, organised crime can be expected to adapt its uptake in line with improvements in these products.

The extent to which firearms and firearm parts are illegally imported into Australia, and are not detected at the border, is currently unknown. Historical trace data has shown proportionally low levels of importation when compared with other known methods of diversion. Increased use of the Internet and darknet websites, however, is likely to drive an increase in firearm importation, and pose a threat to border security (see the case study on page 58).

¹³³ Australian Crime Commission 2014, ‘ACC submission to the inquiry into the ability of Australian law enforcement authorities to eliminate gun-related violence in the community’, ACC, Canberra.

CASE STUDY

DARKNET IMPORTATION OF AN ILLICIT FIREARM¹

In December 2013, a Victorian man was convicted of importing a semi-automatic handgun and possessing ammunition, after the firearm and ammunition magazine were purchased from the darknet website Black Market Reloaded and imported into Australia from the United States, concealed in a karaoke machine.

Although it is not an offence to access darknet websites such as these, it is illegal to import controlled firearms into Australia that have been purchased from these darknet sites.

1 Australian Customs and Border Protection Service 2013, 'Stay out of the firing line of online black markets', ACBPS Newsroom, 14 December 2013, viewed 12 February 2015, <<http://newsroom.customs.gov.au/channels/Firearms-and-weapons/releases/stay-out-of-the-firing-line-of-online-black-markets>>.

The social impacts of firearm trafficking are diverse and include the targeting of legitimate firearm owners and dealers for theft. Some Australian policing jurisdictions saw an increase in the number of registered firearms stolen within their regions in 2013–14.

The Australian Government is aiming to develop a National Firearms Interface (NFI) by 2015, which will track the full life of a firearm, a capacity previously unavailable to law enforcement agencies. This will be achieved through a single shared record for each firearm and for each firearm licensed holder. The NFI allows input of events against a firearm nationally, with visibility of all movements from the time of importation or legal domestic manufacture, including information on status changes, criminal activity, destruction or exportation, thus providing a greater insight into the movement of a firearm.

In February 2015, the Australian Government passed the Crimes Legislation Amendment (Psychoactive Substances and Other Measures) Bill 2014 to introduce international firearms trafficking offences and implement mandatory minimum sentences of five years imprisonment for illegal firearms trafficking. The proposed laws extend the existing offences for cross-border disposal or acquisition of firearms.

High-profile firearm incidents will continue to elevate firearm-related violence to the forefront of public awareness, media headlines and political agendas. The systemic impact of firearm trafficking can include significant government expenditure, and notably legislative change and law enforcement and border protection responses, in an attempt to counter firearm trafficking.

Environmental crime

Australia is a biodiversity haven with pristine natural resources and endangered wildlife. Any organised crime exploitation of the Australian environment is therefore a significant threat.

As with most other crimes, the illicit nature of environmental crime, including the way in which those involved in this market try to commingle legal and illegal commodities and trade, makes it difficult to measure both the extent of environmental crime and the scope of organised criminal involvement in it.

Environmental crime can include:

- illegal trade in wildlife
- illegal harvesting of and trade in timber and other forest products
- pollution caused by the dumping of hazardous waste, illegal discharge and e-waste
- illegal trade in ozone-depleting substances
- illegal, unregulated and unreported (IUU) fishing.

The diverse environmental crime market is often transnational in nature, with international and national environmental experts claiming that it is one of the most profitable and fastest-growing criminal markets.¹³⁴ For example, in 2013 Europol assessed that 1 kilogram of rhino horn was valued at between €37,000 and €46,000, which was nearly twice the price of gold.¹³⁵

Estimates of the value of the global environmental crime market vary widely. For example, the United Nations Environment Programme estimates that organised crime syndicates earn between US\$20 billion and US\$30 billion from environmental crime.¹³⁶ However, the Organisation for Economic Cooperation and Development—while acknowledging the difficulty of quantifying this crime market—estimates the global value to be around US\$30–70 billion. The true value of this crime market is unknown.

¹³⁴ Skinner, E 2011, *Victims of environmental crime—mapping the issues*, International Centre for Criminal Law Reform and Criminal Justice Policy, Vancouver; Bricknell, S 2010, *Environmental crime in Australia*, Australian Institute of Criminology, Canberra; United Nations Environment Programme 2003, *New initiative to combat growing global menace of environmental crime*, 2 June 2003, viewed August 2013, <http://_www.unep.org/Documents.Multilingual/Default.asp?DocumentID=321&ArticleID=4017>.

¹³⁵ Europol 2013, *SOCTA 2013*, Europol, The Hague, p. 57.

¹³⁶ Walters, R 2013, 'Eco mafia and environmental crime', in Carrington, K, Ball, MJ, O'Brien, E & Tauri, JM (eds), *Crime, justice and social democracy*, Palgrave Macmillan, London, pp. 281–94.

A wide variety of actors commit environmental crime, ranging from opportunistic individuals through to sophisticated, well-organised crime groups and corporations. For example, the Australian illicit wildlife market is consistent with international markets and is based on opportunistic activity as well as complex networks involving suppliers, poachers, couriers, collectors and entrenched criminal syndicates.

Wildlife

The illegal wildlife trade in Australia is assessed as a small, niche transnational market. Organised crime groups are attracted to the profits to be made from illegal trade in wildlife, and are most likely to be involved in the high-value transactions.

A limited domestic market, coupled with high international demand for Australian native wildlife, suggests that Australia may be vulnerable to exploitation by both overseas and Australia-based criminal entities seeking to capitalise on this demand.

As well, the Internet is now a key enabler of illegal trade in wildlife, providing an unregulated and anonymous marketplace that introduces suppliers and collectors from around the world.

Illegal logging

Australia has been a destination country for illegal timber and this remains the case. New legislation passed in 2012 is designed to promote the trade in legally harvested timber and timber products. The *Illegal Logging Prohibition Act 2012* (Cwlth) aims to reduce the harmful environmental, social and economic impacts of illegal logging. It is now a criminal offence to import illegally logged timber and timber products into Australia, or to process Australian raw logs that have been harvested illegally.

Hazardous waste

Hazardous waste includes any waste material that is toxic, flammable, corrosive, explosive, infectious or poisonous. Increasingly restrictive regulatory regimes relating to hazardous waste are raising the cost of compliance, providing an opportunity for organised crime to offer low-cost waste disposal solutions to legitimate businesses. This waste is subsequently disposed of illegally by the organised crime groups that provide the service.

Europol has identified both organised crime groups and legitimate businesses involved in the illegal trading of hazardous waste, with some of sufficient size and power to be 'able to participate in large-scale illegal waste management and trafficking activities including manipulating tender processes and disposing of multi-ton amounts of waste'.¹³⁷

Australia is reported to be one of the highest users of technology, making it a source country of e-waste production and vulnerable to illegal domestic dumping of e-waste.¹³⁸ It is likely that Australia will continue to be an exporter of hazardous waste, and e-waste in particular. This, combined with rising regulatory compliance costs, may lead to increased criminal activity in this market.

¹³⁷ Europol 2013, *Threat Assessment 2013*, Europol, The Hague, November 2013, p. 10.

¹³⁸ Australian Bureau of Statistics 2013, 'Waste generated per person', from *Measures of Australia's Progress 2010: is life in Australia getting better?*, ABS, Canberra, viewed 12 March 2015, <[http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1370.0~2010~Chapter~Waste%20per%20person%20\(6.6.3\)>](http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1370.0~2010~Chapter~Waste%20per%20person%20(6.6.3)>).

Ozone-depleting substances

The Montreal Protocol on Substances that Deplete the Ozone Layer is the global protocol that sets out a mandatory timetable for the phasing out of ozone-depleting substances. Ratified by 196 countries, the Montreal Protocol sets binding progressive phase-out obligations for developed and developing countries for all the major ozone-depleting substances, including chlorofluorocarbons, halons and less damaging transitional chemicals such as hydrochlorofluorocarbons. According to the protocol, all ozone-depleting substances are to be phased out by 2030.

It is unclear if there is an illicit ozone-depleting substances market in Australia. However, globally, an illegal trade in ozone-depleting substances has been observed since the Montreal Protocol came into being. A recent United Nations Office on Drugs and Crime (UNODC) assessment¹³⁹ noted that the Montreal Protocol had created conditions for an ozone-depleting substances black market, and that the trade exhibited evidence of transnational criminal networks spanning different continents and nationalities.

Illegal, unregulated and unreported fishing

IUU fishing refers to fishing that does not comply with national, regional or global fisheries conservation and management obligations. IUU fishing occurs in Australian waters when either domestic or foreign fishing vessels contravene Australian fishing laws and regulations. Deterrents, including surface and air surveillance, together with a national commitment to pursue infringements, will probably continue to keep this illegal activity at a low level.

Internationally, law enforcement agencies are increasingly acknowledging the significance of transnational environmental crime (including the resultant harms), as well as the involvement of organised crime. The UNODC, Europol and INTERPOL have all initiated projects, resolutions or threat assessments to address environmental crime. For example, since late 2011, INTERPOL has developed five projects covering different elements of environmental crime. Two of these projects—Project Eden, targeting the illegal trading and disposal of waste, and Project Scale, which aims to detect, suppress and combat fisheries crime—were initiated in 2013. The European Union Serious and Organised Crime Threat Assessment 2013 also identified environmental crime as one of the emerging threats requiring intensified monitoring.

The direct harm from environmental crime is damage to the environment and wildlife. Environmental crime damages the environment by polluting and depleting natural resources and by compromising the survival of native and introduced flora and fauna. Environmental harm also damages the health of communities and individuals and has a detrimental effect on stability of the labour market in tourism, environment and sustainable industries.

¹³⁹ United Nations Office on Drugs and Crime 2013, *Transnational organized crime in East Asia and the Pacific: a threat assessment*, UNODC, Vienna, April 2013.



CRIMES IN THE MAINSTREAM ECONOMY

Card fraud

Card fraud is defined as the fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain.

Card fraud may involve:

- application fraud—the acquisition of legitimate cards from financial institutions by using false supporting documentation
- card theft or card-not-received fraud—the theft of legitimate credit and debit cards before the designated customers receive them
- card-not-present fraud—the use of acquired card details to make purchases over the phone or Internet, so the card does not need to be physically presented
- card skimming—the illegal copying of card details from a card's magnetic stripe at automatic teller machines (ATMs) or at point of sale, which can then be used to create counterfeit cards
- the creation and use of counterfeit cards—the production and use of fake credit cards, with card details skimmed or acquired from the legitimate cards of unsuspecting victims
- phishing—the acquisition of customer card or account details through deceptive emails aimed at tricking the customer into providing information to enable illegal account access
- hacking—the acquisition of personal and account details by gaining illegal access to company databases to steal customer financial data.

The card fraud market continues to be dominated by overseas-based groups. Many groups are based overseas and travel to Australia to conduct specific card fraud offences—for example, conducting shopping trips with fraudulent cards or skimming ATMs for card details.

Card-not-present fraud

The incidence of card-not-present fraud continues to rise, and it is the most prominent form of card fraud, reportedly accounting for 72 per cent of all card frauds in Australia in 2013. The Australian Payments Clearing Association (APCA) reported a rise in card-not-present fraud on Australian cards in the 2013–14 financial year, from A\$199.2 million to A\$256.1 million. Sixty-six per cent of this fraud on Australian cards occurred overseas.

Over the four years until December 2013, there was a 67 per cent increase in card-not-present fraud, which may be in parallel with the 140 per cent growth in online shopping over the same period.¹⁴⁰

Skimming

APCA reports that counterfeit/skimming fraud has increased from A\$37.0 million to A\$42.0 million over the 12 months to June 2014. However, this is still much lower than the peak of A\$66.0 million in 2011. This increase is reported to be influenced by the rise in the incidence of ATM skimming over the period.¹⁴¹

Lost/stolen card fraud

APCA has also reported that lost and stolen card fraud on Australian cards increased from A\$30.5 million to A\$33.1 million over the 2013–14 financial year. The majority of this increase is attributable to fraud taking place on Australian cards used in overseas banking systems; however, fraud occurring on Australian cards used within the Australian banking system has decreased.¹⁴²

Australia is one of the countries leading the adoption of contactless payments. The system was introduced as recently as 2007, but there are now about 100 million contactless payments on credit/debit cards every month. The rapid uptake of contactless payments in Australia is likely to attract serious and organised crime groups involved in card fraud. Contactless payments are more secure than magnetic stripe card technology, which remains an easy and lucrative way to facilitate serious and organised card fraud. However, with the gradual phasing out of magnetic stripe technology, the exploitation of contactless payments will become more attractive to serious and organised crime.

¹⁴⁰ Australian Payments Clearing Association 2014, 'Payments fraud trends a reminder to take care when Christmas shopping online', media release, 9 December 2014, viewed 8 January 2015, <<http://apca.com.au/docs/2014-media-releases/Payments-fraud-trends-a-reminder-to-take-care-when-Christmas-shopping-online.pdf>>.

¹⁴¹ *ibid.*

¹⁴² *ibid.*

Mail theft

In the past two years, the incidence of theft of cards from the mail has increased, with a particular increase observed since early 2013. It is possible that improved security measures such as card chip and personal identification number (PIN) security have led less-sophisticated criminal entities to revert to stealing genuine cards. The introduction of contactless payment cards may also have led to an increase in less-sophisticated criminals stealing cards from the mail. The ability to use these cards to purchase goods without having to provide a PIN or signature leaves them susceptible to small-scale card fraud, as transaction and daily amount limits reduce the potential for large-scale fraud.

Technology

Technology is a significant enabler of card fraud, facilitating both the theft of details and the sale of fake cards and personal information. Advances in technology continue to influence how card fraud is conducted. The ability of organised crime to hack into corporate datasets and steal banking details remains a key threat. As the amount of personal information placed or stored online increases, this threat is likely to increase.

Darknets continue to facilitate card fraud. One site identified by law enforcement in Australia was selling cards for 8 cents, card code verifications (CCVs) for \$8, and other card details, including billing addresses, for \$80. At one point, 14,000 users were known to be accessing the site.

Technology-based improvements in ATM, EFTPOS and card security will also continue to influence card fraud methodologies used by serious and organised crime groups. As technology continues to enhance security features, organised crime will develop countermeasures. Organised crime groups that remain involved in card skimming are displaying increased sophistication in their methodologies. For example, they are now installing skimming devices within ATMs that are not detectable by either the customer or the ATM owner. Criminal groups are also targeting specific service industries to compromise card data.

The use of Internet-capable mobile devices to conduct financial transactions has increased over recent years and will continue to increase. This increased use, combined with expanded device functions, such as the capability to conduct Internet banking and other online transactions, is likely to be exploited by organised crime.

Although APCA has assessed that the card fraud rate in Australia was one-third less than that of the United Kingdom in 2013,¹⁴³ assessments of the size of the card fraud market based on reported card fraud figures are likely to underestimate the market size. Individuals who have been the victim of card fraud report that fraud to their financial institution rather than to police, and these financial institutions are reluctant to provide details of their full exposure to card fraud. Independent surveys may present a more accurate assessment. In one survey conducted in late 2012, 31 per cent of Australian respondents indicated that they had been a victim of card fraud in the previous five years.¹⁴⁴

¹⁴³ *ibid.*

¹⁴⁴ Inscoe, SW 2012, *Global consumers react to rising fraud: beware back of wallet*, Aite Group LLC, Boston.

Though individuals can be inconvenienced financially by card fraud, more enduring harm may be caused to personal credit ratings, identity and privacy. This may extend to emotional stress and fears for personal safety.

Card fraud, while harming the banking sector in the first instance, ultimately harms bank customers to whom the losses associated with card fraud are passed on as increased costs for banking services. Card fraud also damages commercial reputations and can disrupt business operations when payment facilities or information technology systems are compromised, particularly by skimming or hacking. Furthermore, card fraud can increase business costs and make the allocation of resources more complex or more burdensome for a business when it seeks to balance the uptake of anti-fraud practices against other operational priorities.

Revenue and taxation fraud

Revenue and taxation fraud involves the intentional and dishonest evasion of taxation obligations. The Australian Taxation Office (ATO) is responsible for the administration of tax products, which include income tax, goods and services tax (GST) and excise. Revenue and taxation fraud has the potential to reduce revenue collected and refunds paid, undermine self-assessment and voluntary compliance, which underpins the taxation system, and affect public confidence in the integrity of tax administration.

Organised crime entities exploiting the Australian taxation system are increasingly using complex and sophisticated organisational structures, making these entities less recognisable and harder to detect. There are four main ways in which organised crime perpetrates revenue and taxation fraud in Australia:

- tax refund fraud
- tax evasion schemes
- phoenixing schemes
- abusive use of trust structures.

There is clear evidence of the involvement of organised crime groups in the commission of tax refund fraud, including the emergence of transnational elements.

Examples of identified organised crime involvement in fraud on the taxation system are:

- large-scale property development projects involving multiple GST-registered businesses conspiring together to defraud the GST system through a series of false invoices
- exerting influence over tax agents and illegally accessing tax agent systems and information to perpetrate fraud
- attacks through the tax agent portal
- an increase in the theft of information from tax agents and employers (as reported to the ATO by those affected), where this information can be used for Business Activity Statement refund fraud and false payment summaries used for income tax fraud

- the provision of labour hire services to industries using invalid contractor arrangements and unsubstantiated or exaggerated claims to avoid tax and other employer obligations, coupled with phoenix-like tactics in an attempt to avoid compliance action
- the lodging of false or fraudulent tax refund claims.

Refund fraud is very frequently enabled by identity crime. In particular, organised crime groups involved in revenue and taxation fraud have been lodging false returns that use the identities of those who have entered Australia on short-term visas.

Organised crime groups continually adapt their business models to explore low risk, high profit opportunities, including the use of sophisticated information technology expertise to perpetrate extensive attacks on information contained in government systems. These sorts of cyber attacks are aimed at harvesting taxpayer details such as tax file numbers and Australian Business Numbers, or at gaining illicit access to tax agent portals to perpetrate taxation fraud.

Professional facilitators working on behalf of organised crime remain a risk, with criminally 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 ATO.

Offshore tax evasion and fraud arrangements are becoming more complex, involving multiple layers of entities, havens and funds flows (see the case study on page 67). These arrangements are intended to illegally reduce taxable income, increase tax deductions against income, or avoid tax entirely. Professional facilitators, such as accountants and solicitors, are particularly valuable to organised crime and high-net-worth individuals in implementing these schemes.

Fraudulent phoenix activity also threatens the integrity of the tax revenue and superannuation systems. Phoenix fraud occurs when a company is intentionally placed into administration or liquidation to avoid payment of taxes and superannuation guarantee and/or other employee entitlements. A new company is then created to carry on the same or a similar business, typically with the same ownership. Fraudulent phoenixing activities deprive the community of necessary funds for essential services, and provide phoenix operators with an unfair competitive advantage over businesses operating legitimately in the same sector and meeting their tax and employee entitlement obligations.

The ATO reports that many of the individuals associated with fraudulent phoenix companies are known to be, or are suspected of being, criminals and/or are associated with criminal organisations spanning state, territory and sometimes national boundaries.

CASE STUDY

USE OF OFFSHORE ENTITIES TO EVADE TAX FROM THE SALE OF AUSTRALIAN STOCK EXCHANGE (ASX)-LISTED SHARES

Australian taxpayers who were clients of a well-known promoter used the services of an offshore service provider (OSP) located in Samoa to create controlled entities in jurisdictions such as Samoa, the British Virgin Islands, Cayman Islands, Gibraltar, Singapore, Switzerland, Ireland and the United Kingdom in an attempt to obfuscate residency status, and to create layers between share trading profits and beneficial ownership. The promoter used the services of Samoan entities, including a private bank and a trust, to establish entities on behalf of clients in these jurisdictions.

These entities provided nominee shareholders and directors to conceal true ownership and traded on the ASX on behalf of their nominees. Funds were often 'parked' overseas in the guise of insurance products, using the services of an offshore insurance company. When funds were repatriated, it was in the guise of loans, which were also used to generate false deductions for interest expenses. Loan draw-downs equalled the amount of interest payable.

67

Abusive trust fund schemes continue to be used by organised crime to hide criminal wealth, with the key advantage of trusts being their lack of transparency to regulators, allowing the beneficial owners of the funds in trusts to remain anonymous.

The harm from revenue and taxation fraud can be measured in the amount of tax dollars forgone to national revenue collection. Although this makes the government the ostensible victim of revenue and taxation fraud, revenue and taxation fraud affects the entire Australian community, reducing the tax revenue available to provide government-funded public services, including infrastructure, transport, health services and education.

The tangible harms of revenue and taxation fraud are therefore measured less in dollars and more in the level of resources ultimately available to support societal wellbeing and social organisation.

Illegal tobacco

Organised crime remains entrenched within the illegal tobacco market in Australia. It continues to perceive involvement in this market as a low risk, high profit enterprise.

The illegal tobacco market in Australia is supplied almost entirely by overseas-sourced product. Tobacco being smuggled into Australia to supply the illegal tobacco market comes in three forms:

- unbranded ('chop chop')—illicit tobacco sold as loose leaf or in tubes
- counterfeit—a copy of a particular product, carrying a trademark without the permission of the trademark owner, and sold for a price much lower than the legal product
- contraband—any cigarettes, counterfeit or legal, imported illegally and sold without the payment of applicable duties.

Included in the category of contraband are 'cheap whites', also known as 'illicit whites'. These are cigarettes that have been produced legally in a factory with the approval of a licensing authority in an overseas jurisdiction, but that do not meet the product standards required in the jurisdiction in which they are eventually sold. Legitimate tobacco companies operating in the legal tobacco market in Australia have claimed that 'illicit whites' are a rapidly growing feature of the illegal tobacco market, with the Manchester brand the largest illicit white brand in Australia.

All of the three forms of tobacco product, when smuggled into Australia without duty being paid, are illegal. Organised crime seeks to make a significant profit from the importation of both genuine and counterfeit product.

Sea cargo has traditionally been the primary importation method (see the case study on page 69). In 2013–14, there was an increase of almost 7 per cent in the number of detections of illegal tobacco through this stream. However, the equivalent in total weight of tobacco seized from sea cargo had decreased by about 14 per cent: 296 tonnes in 2013–14, down from 343 tonnes in 2012–13. At the same time, there was a significant increase in the number of detections of undeclared cigarettes through the international mail and air cargo streams. The decrease in the total weight of detections in sea cargo during this period indicates a shift in smuggling methodology, where there is a corresponding increase in detections through the air and postal streams of smaller, more frequent shipments.¹⁴⁵ There are indications that those groups involved in the market are highly networked and that they have made significant effort to gain a knowledge of Customs procedures, priorities and detection limitations.

¹⁴⁵ Australian Customs and Border Protection Service 2013, *Annual Report 2013–14*, ACBPS, Canberra, pp. xi, 26.

CASE STUDY

SEIZURE OF 2 TONNES OF ILLICIT TOBACCO¹

In September 2014, the Australian Customs and Border Protection Service seized about 2.2 tonnes of undeclared loose tobacco, located in a sea cargo container entering Australia at the Port of Melbourne.

The illegal tobacco was concealed in aluminium foil packages labelled 'Pandan Tea' and originated in Vietnam. The revenue that would have been evaded by this attempted illegal importation is estimated at almost A\$1.5 million.

¹ Australian Customs and Border Protection Service, 'ACBPS stops over two tonnes of illicit tobacco at the border', ACBPS Newsroom, 18 September 2014, viewed 12 February 2015, <<http://newsroom.customs.gov.au/releases/acbps-stops-over-two-tonnes-of-illicit-tobacco-at-the-border>>.

Since the closure of the legal domestic tobacco production industry in 2006, there has been an ongoing decline in the supply of domestically grown tobacco to the illegal market. However, in May 2014, the Australian Taxation Office Operation Garnet search warrants, with the assistance of the Australian Federal Police, resulted in the largest-ever seizure of illegal locally grown tobacco, located in regional Victoria. About 350,000 mature tobacco plants were seized, which were estimated to have an excise value of A\$15 million.¹⁴⁶

It is highly likely that the illegal tobacco market will remain attractive for serious and organised crime groups because of the very large profits that can be made with very low risk.

Tobacco consumption is widely recognised as a major cause of preventable death and disease in Australia, with smoking responsible for more drug-related hospitalisations and deaths than alcohol and illicit drugs combined.¹⁴⁷ Smoking is known to greatly increase the risk of many cancers, cardiovascular disease, chronic obstructive pulmonary disease and other respiratory diseases, peripheral vascular disease and many other serious medical conditions. Exposure to second-hand smoke also causes disease and premature death in adults and children who do not smoke.

¹⁴⁶ Australian Taxation Office 2014, 'ATO rolls illegal tobacco', media release, 4 May 2014, viewed 8 January 2015, <<https://www.ato.gov.au/Media-centre/Media-releases/ATO-rolls-illegal-tobacco>>.

¹⁴⁷ Department of Health and Ageing 2012, *National Tobacco Strategy 2012–2018*, DOHA, Canberra.

Superannuation fraud

Australia's very large pool of compulsory superannuation savings, totalling A\$1.62 trillion,¹⁴⁸ makes it an attractive target for organised crime. The superannuation industry in Australia encompasses a complex array of fund types, ranging from 'do-it-yourself' funds—or self-managed superannuation funds (SMSFs), which are regulated by the Australian Taxation Office (ATO)—to large industry and retail funds that are overseen by the Australian Prudential Regulation Authority (APRA). Because of the inherent complexities of this industry, a range of opportunities exist for fraud, including the theft of contributions and fund assets, fraudulent fund investments, non-existent schemes and excessive fees charged by advisers.

There are a number of factors that make the Australian superannuation sector particularly attractive to organised crime:

- There is a very large pool of compulsory superannuation savings, with an incremental increase in compulsory contributions to 12 per cent due by 2019.
- Many Australians are disengaged from their superannuation, rarely checking the balance or performance of their fund, which increases the risk that detection of any fraud will only occur upon retirement.
- The complex nature of superannuation regulation in Australia, in which different regulatory bodies, including the Australian Securities and Investments Commission (ASIC),¹⁴⁹ APRA and the ATO all have separate and distinct roles, makes it difficult to trace malfeasance in the sector.

The Australian superannuation industry is broadly segmented into funds regulated by APRA, including industry funds, corporate funds, retail funds and public sector funds, and SMSFs regulated by the ATO. Sixty per cent (or A\$970 billion) of the total Australian superannuation industry investments are held in APRA-regulated funds, while A\$506 billion or 31 per cent are held in SMSFs and the remainder are in public sector funds and other schemes.¹⁵⁰

These investments are equivalent to about 120 per cent of the Australian share market capitalisation and 90 per cent of Australia's annual gross domestic product (GDP).¹⁵¹

Australian superannuation is expected to achieve continued growth as a result of the tax advantages pertaining to it and the compulsory nature of the Superannuation Guarantee, and will accumulate almost A\$7 trillion (130 per cent of GDP) over the next 25 years.¹⁵²

¹⁴⁸ As at 9 January 2014.

¹⁴⁹ ASIC's role in connection with the superannuation industry is in relation to regulation of the licensing of financial service providers.

¹⁵⁰ Australian Prudential Regulation Authority 2014, *Annual Superannuation Bulletin, June 2013*, issued 9 January 2014, viewed 13 January 2014, <<http://www.apra.gov.au/Super/Publications/Documents/Revised%202013%20Annual%20Superannuation%20Bulletin%2005-02-14.pdf>>.

¹⁵¹ KPMG 2012, *Evolving superannuation industry trends*, November 2012, viewed 16 December 2013, <www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/evolving-superannuation-industry-trends.pdf>.

¹⁵² Australian Government Budget 2012–13, *Budget Paper*, viewed 16 December 2013, <www.budget.gov.au/2012-13/content/bp1/html/bp1_bst4-03.htm>.

Therefore the Australian superannuation industry is a major contributor to the Australian financial sector and is a source of wealth attractive for targeting by opportunistic individuals and organised crime.

Some of the organised crime networks identified as targeting the Australian market have committed similar frauds in numerous overseas jurisdictions and—because of their complex global networks of professional advisers, their level of sophistication and their ability to adapt their activities in line with regulatory changes—have remained resistant to law enforcement and regulatory agency intervention.

Traditionally, SMSFs have been more attractive for fraudulent exploitation than APRA-regulated funds as they are self-managed and not prudentially regulated, with ultimate responsibility and risk associated with investments residing with individual trustees and members. The fact that SMSFs hold, on average, the largest balance of superannuation assets provides an opportunity for low-volume, high-impact fraud on individual funds that may be managed by financially inexperienced individuals.

The defrauding of SMSFs aside, these fund types may also be attractive to organised crime as a vehicle for money laundering, as criminals can easily mask large transfers into their funds as ‘legitimate’ investment activity. However, the effectiveness of SMSFs as an investment vehicle to launder significant amounts of funds is limited by contribution caps and benefit payment restrictions.

Recent investigations and intelligence have shown particular similarities in the commission of superannuation frauds. These include:

- the use of trusted professionals such as financial planners, who are complicit in the fraud
- the deliberate use of investment structures that are complex, multi-layered and opaque, and in foreign jurisdictions
- increased use of technology and cybercrime
- the resilience of the syndicate to international law enforcement and regulatory agency intervention.

The need for individuals to rely on professional advisers in the superannuation sector continues to grow because of ongoing increases in the complexity of the rules and regulations affecting this sector. These advisers are at risk of being exposed to coercion or exploitation by organised crime because of their in-depth knowledge of the industry and their ability to exploit loopholes in controls.

As SMSFs and APRA-regulated superannuation funds transition more to the online environment, there is potential for superannuation funds to fall victim to high-tech crime. With online processing systems, superannuation funds may fall victim to phishing and key logging scams. Cloud computing and storage of the financial details of individuals in the cyberspace environment may also represent a risk.

Stronger Super reforms commenced in July 2013 and included a number of reforms to strengthen the governance, integrity and regulatory settings of the superannuation system, with particular focus on SMSFs. The reforms included measures to give the ATO powers to address wrongdoing and non-compliance by SMSF trustees, capturing rollovers to SMSFs as a designated service under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*, and establishing a register of SMSF auditors (administered by ASIC).

Further, regulatory safeguards such as the SMSF Member Verification System initiatives provide more certainty and transparency in the SMSF registration and rollover process. This is in addition to recent enhancements to the ATO's registration and screening systems and the provision of specific instructions from APRA to funds on rollover procedures. These reforms have significantly reduced instances of large-scale illegal early release schemes conducted using SMSFs.

Because of the large amount of funds involved, infiltration of the Australian superannuation system by organised crime, and the associated losses through fraudulent activity, would result in more people relying on the social security system in their retirement. With the Australian tax base supported by a lower proportion of workers compared with retirees, significant increases in the demand for government pensions would have serious economic implications for the government.

Significant and continued financial losses in this sector could also lead to a lack of confidence in the Australian financial system broadly, and in superannuation in particular, leading to a withdrawal of investors from the sector.

Investment and financial market fraud

Australia remains an attractive target for domestic and overseas-based organised crime involved in investment and financial market fraud because of its comparatively stable economy and Australian investors' high subscription to share purchases.

Further, the movement of organised crime in Australia from traditional illicit markets such as drugs to the investment and financial fraud market may be attributable to a perceived lower risk of detection and the substantial illicit profits to be earned.

Investment and financial market fraud, in the context of this report, refers collectively to the following types of frauds that target Australians:

- fraudulent investment schemes, such as boiler-room fraud¹⁵³ (also called cold-call investment fraud) and Ponzi schemes,¹⁵⁴ which attract victims with promises of high financial returns and claims of low risk investment strategies

¹⁵³ Boiler-room fraud refers to the unsolicited contacting of potential investors who are deliberately given fraudulent, false, misleading or deceptive information designed to entice them to buy, sell or retain securities or other investments.

¹⁵⁴ A Ponzi scheme is a type of fraud that uses money from new investors to make interest payments to earlier investors. These schemes typically offer high rates of return and fail when no new investors can be found.

- 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’¹⁵⁵ schemes
- exploitation of financial securities¹⁵⁶ to commit fraud or launder or conceal the proceeds of crime—for example, off-market share transfers and fraudulent share schemes.

Investment fraud

Investment fraud can be a complex, sophisticated and transnational activity that generates significant illicit profits with minimal risk of disruption, making it attractive to organised crime.

The extent of organised crime involvement in investment fraud, such as boiler-room activity, targeting Australia remains difficult to determine, particularly where those groups are based offshore. Compounding this difficulty is the fact that victimisation from investment fraud is understood to be under-reported, as victims either are too embarrassed to report their losses or do not realise that they have been defrauded. It is noted that some boiler-room frauds promote investment in fraudulent superannuation schemes or defraud individuals of money that they invest under the auspices of their self-managed superannuation funds (SMSFs).

Task Force Galilee¹⁵⁷ found that the Australian victims of boiler-room investment frauds saw the schemes as attractive because of the economic climate at the time, in which returns on traditional investments, such as Australian shares and property, were very low and investors were seeking higher-yielding investment opportunities.

The majority of investment fraud, such as boiler-room activities, targeting Australians is currently understood to be perpetrated from bases offshore. A new domestic investment fraud threat however, has recently been identified. Although law enforcement investigations have traditionally shown that organised criminal entities promoting fraudulent investment schemes in Australia do so without holding an Australian Financial Services (AFS) licence,¹⁵⁸ in recent cases, organised crime entities have been identified seeking to obtain AFS licences in order to give an appearance of legitimacy to an illegal undertaking. 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’.

¹⁵⁵ A ‘share ramping’ or ‘pump and dump’ scheme involves the use of false and misleading information to generate investor trading interest to ‘pump’ up the price of a company’s shares. These schemes differ from classic market manipulation because of the use of false and misleading information to affect share prices. The schemes differ from insider trading as they do not involve the illegal use of inside information.

¹⁵⁶ The large numbers of securities on offer in Australia include shares, bonds, derivatives and managed funds.

¹⁵⁷ Task Force Galilee was a multi-agency taskforce established to combat and prevent serious and organised investment fraud targeting the Australian community.

¹⁵⁸ In order to provide financial services to Australian residents, the provider of the services must hold an AFS licence issued by ASIC or be an authorised representative of a holder of an AFS licence.

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.

Sectors and industries, such as the mining and resources sector and the biotech and pharmaceutical industries, are vulnerable to investment fraud backed by organised crime. One of the attributes of these sectors and industries that make them attractive for infiltration by organised crime involved in investment fraud is the speculative nature of capital raisings. Because of the number of years that it can take from proof of concept stage to establishing a viable operation, it is very difficult for investors to determine whether or not a promoted product is fraudulent.

Financial market fraud

Recent law enforcement investigations indicate that organised crime is increasingly involved in financial market fraud. Some of these frauds are transnational, with separate networks in different jurisdictions.

Project Wickenby¹⁵⁹ investigations have increased the level of understanding of the risks posed to Australian investors by the abusive use of the securities market and secrecy jurisdictions. Of primary concern is the opacity of the beneficial ownership of Australian-listed shares, which provides the opportunity for organised crime entities to hide their involvement in fraudulent and other illegal activities, including money laundering and tax evasion.

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 United States Commodity Futures Trading Commission reports that it has witnessed a sharp rise in foreign exchange trading frauds in recent years. The perpetrators of these frauds have been seen to use 'wealth creation' webcasts, webinars, podcasts, emails and other online seminars on the Internet to solicit clients worldwide. One scheme in particular accepted at least US\$53 million from at least 960 clients worldwide, including investors in Australia.¹⁶⁰

Globalisation and innovation will continue to result in the creation of new investment products, services and technologies that may be used to facilitate investment and financial market fraud in the future.

¹⁵⁹ Project Wickenby is a cross-agency taskforce designed to strengthen national law enforcement and Australian Taxation Office (ATO) compliance activities against taxation fraud. Led by the ATO, Project Wickenby includes the Australian Crime Commission, the Australian Federal Police, the Australian Securities and Investments Commission, the Attorney-General's Department, the Australian Transaction Reports and Analysis Centre, the Australian Government Solicitor and the Commonwealth Director of Public Prosecutions.

¹⁶⁰ United States Commodity Futures Trading Commission, Release: PR6353-12, 19 September 2012, viewed 9 January 2014, <<http://www.cftc.gov/PressRoom/PressReleases/pr6353-12>>.

Investment and financial market fraud can undermine the integrity and reputation of financial markets and discourage international investment in Australian securities, which in turn adversely affects the Australian economy.

At the social level, harm is caused by the financial hardship incurred when victims are manipulated to invest their money in a fraud. The end result for victims can include chronic financial insecurity; depletion of personal wealth; sudden reliance on welfare; housing problems and even homelessness; mental illness; and, in extreme cases, self-harm and suicide. Investors who lose money that is uncompensated may come to lack confidence in the financial system and distrust government and regulators, and may be less likely to participate in the financial system in the future, which also has an impact on the economy.

Visa and migration fraud

Visa and migration fraud is an illicit market that has not previously been addressed in *Organised Crime in Australia 2013*. Collaborative work between the Australian Crime Commission and the Department of Immigration and Border Protection has identified that organised crime has infiltrated and exploited the visa and migration fraud market, and will continue to do so. Visa and migration fraud may be linked to human trafficking or maritime people smuggling, both of which are dealt with in the 'Crimes against the person' section of this report.

Visa and migration fraud occurs when a visa is issued on fraudulent or false grounds. It occurs in two main forms:

- The use of legitimate visas obtained fraudulently—where visa recipients, or agents acting on their behalf, make false claims to meet visa requirements. Both permanent and temporary visa classes are used to gain unlawful entry into Australia, including partner visas, Electronic Travel Authorities, skilled temporary migration (457) visas, student visas, working holiday makers and tourist visas.
- The use of illegitimate or illegal visas and passports (document fraud).

Visa and migration fraud can be complex, systemic and organised, involving a range of complicit individuals—including the applicants themselves—and other entities such as registered migration agents and business operators.

Significant profits can be made from visa and migration fraud, with facilitators arranging entry to and/or stay in Australia on visas obtained on fraudulent or false grounds. Organised crime groups and other known criminal entities are exploiting vulnerabilities associated with some visa subclasses, and are using false or fraudulent documentation to fulfil visa requirements. Visa and migration fraud is being used by organised crime as a means of obtaining cheap labour and potentially expanding their criminal networks; this is done by facilitating unlawful entry, visa extensions and employment for individuals, while extorting, underpaying and exploiting employees.

Some registered migration agents use their detailed knowledge of Australian visa and migration processes to exploit vulnerabilities in the system to facilitate unlawful entry into Australia, and make significant profits by charging inflated fees for services.

Visa and migration fraud has the potential to pose a significant threat to Australia's migration system. It is also a possible threat to Australia's national security, given that true identities are often difficult to establish when individuals arrive in Australia with fraudulent documentation and false identities.



CRIMES AGAINST THE PERSON

Human trafficking and slavery

Human trafficking is the act of recruiting, transporting, transferring, harbouring or receiving a person by means of the threat or use of force, deception, coercion or abuse of power, for the purpose of exploitation, including sexual and labour exploitation, and the harvesting of body organs.

Human trafficking is a very different crime from people smuggling. In Australia the term 'human trafficking and slavery' is used to encompass a range of crimes, including those in which a person is moved domestically or transnationally for the purposes of exploitation, as well as those in which a person already in Australia is subjected to exploitative practices such as slavery and slavery-like practices, including servitude, forced labour and forced marriage. The link between these crimes is that a person's freedom and ability to make choices for themselves are substantially constrained, whether that is because of the use of coercion, threat or deception, or because the powers of 'ownership' have been exercised over them. In contrast, people smuggling is the organised, irregular movement of people across borders, usually on a payment-for-service basis, and does not usually involve the ongoing exploitation of the victim by the offender.

The clandestine nature of human trafficking, along with probable high levels of under-reporting and low levels of recognition, including through self-identification, means that there is little reliable data about the nature and extent of human trafficking at a global, regional or domestic level. However, there is general consensus that human trafficking affects almost every country in the world, whether as a source, transit or destination country, or as a combination of these.

Opportunities to traffic people into, or exploit people within, Australia are curtailed by strong migration controls, geographic isolation and a high degree of regulation, compliance and enforcement. Australia's comprehensive whole-of-government strategy to combat human trafficking and slavery also helps to ensure that Australia is a hostile environment for offenders. However, Australia is traditionally a destination country for people trafficked from Asia—particularly from Thailand, the Republic of Korea and Malaysia—and is potentially a source country in relation to forced marriage.

Historically, the majority of human trafficking and slavery matters investigated in Australia have related to women working in the sex industry. However, in recent years, cases of men and women exploited in a range of other industry sectors—such as hospitality, agriculture and construction—have increasingly been identified. In 2013–14, 35 per cent of investigations conducted by the Australian Federal Police (AFP) related to forms of labour exploitation not involving the sex industry. Of the 21 clients referred to the Support for Trafficked People Program in 2013–14, 62 per cent experienced exploitation other than in the sex industry.¹⁶¹

In 2013–14, the AFP commenced 10 new investigations relating to forced marriage. Three of these investigations related to marriages that had already taken place. Operational evidence has shown that forced marriage matters require a different investigative approach from other human trafficking and slavery matters. The forced marriage referrals received to date have primarily involved Australian citizens under the age of 18, with relatives alleged to have arranged, or to be arranging, a marriage for them overseas without their full and free consent.¹⁶²

Maritime people smuggling

The United Nations High Commissioner for Refugees (UNHCR) reported that at the end of 2013 there were 51.2 million forcibly displaced people worldwide, including 33.3 million people internally displaced¹⁶³ as the result of conflict.¹⁶⁴ Internally displaced people are targets for people smugglers worldwide, and in recent years Australia has been seen as an attractive destination because of its geographic location and positive economic, political and social environment. It is also one of the few countries in the region that is a signatory to the Refugee Convention.¹⁶⁵

¹⁶¹ Australian Government 2014, *Trafficking in persons: the Australian Government response, 1 July 2013–30 June 2014*, Sixth Report of the Interdepartmental Committee on Human Trafficking and Slavery, Australian Government, Canberra.

¹⁶² *ibid.*

¹⁶³ For the purposes of United Nations statistics, internally displaced persons are people or groups of individuals who have been forced to leave their homes or places of habitual residence as a result of armed conflict and who have not crossed an international border.

¹⁶⁴ United Nations High Commissioner for Refugees 2014, *UNHCR global trends 2013* (online), viewed 23 January 2015, <<http://unhcr.org/trends2013/>>.

¹⁶⁵ Crock, M & Ghezelbash, D 2010, 'Do loose lips bring ships?', *Griffith Law Review*, vol.19, no. 2, pp. 238–87.

There are only two possible means of entry into Australia—by air or by sea. People smuggling occurs through both streams, but people smuggling by air is more difficult, as it generally requires some form of fraudulent documentation, access to corrupt officials en route, or both.¹⁶⁶ The most visible form of people smuggling to Australia occurs by sea. Maritime people smuggling is usually one stage of a much larger journey, also involving land and air movements.¹⁶⁷

Maritime people smuggling voyages are particularly dangerous and have resulted in substantial loss of life at sea. Conditions during the journey may be crowded and a lack of hygiene on board can result in the spread of disease.¹⁶⁸ Journeys may require travel through rough seas in boats that are unseaworthy, sinking without the means for passengers (who may not have been provided with life vests) to signal for help.¹⁶⁹

Maritime people smuggling is generally viewed as a high profit and low risk venture¹⁷⁰ because of the relatively low risk of detection, arrest and prosecution compared with other activities undertaken by transnational organised crime groups.¹⁷¹ It is generally carried out by flexible criminal groups or individuals, operating in repeated contractual arrangements, rather than in structured hierarchies.¹⁷²

At the peak of maritime people smuggling activity in 2012 and 2013 (see Table 2), high demand meant that illegal maritime arrivals (IMAs) on board suspected illegal entry vessels (SIEVs) were well served by established people smugglers and a few opportunists. However, the countermeasures implemented under the Regional Resettlement Agreement and Operation Sovereign Borders have effectively suppressed that demand.

Table 2: SIEVs and IMAs by calendar year, 2008–2015¹⁷³

Year	Number of SIEVs	Number of IMAs (excluding crew)
2008	7	161
2009	55	2,574
2010	138	6,650
2011	70	4,622
2012	276	17,072
2013	302	20,719
2014	1	168
2015 (as at 28/02/2015)	0	0

¹⁶⁶ Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.

¹⁶⁷ *ibid.*

¹⁶⁸ United Nations Office on Drugs and Crime 2011, Issue paper: smuggling of migrants by sea, UNODC, Vienna.

¹⁶⁹ *ibid.*

¹⁷⁰ Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.

¹⁷¹ INTERPOL Fact Sheet, People smuggling, <<http://www.interpol.int/Crime-areas/Trafficking-in-human-beings/People-smuggling>>.

¹⁷² United Nations Office on Drugs and Crime 2011, Issue paper: smuggling of migrants by sea, UNODC, Vienna.

¹⁷³ Data provided by Australian Customs and Border Protection Service.

On-water operations, intergovernmental cooperation, regional processing centres and strategic messaging campaigns have convinced most potential illegal immigrants not to join a maritime venture to Australia. Despite the results under Operation Sovereign Borders, the maritime people smuggling threat is enduring.

Child sex offences

Organised child sex offending in Australia is different from that seen in other countries, particularly in South East Asia and Eastern Europe. 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 a 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.

The true extent of child sexual abuse in Australia is unknown, although statistics can give some insight. In 2012, there were 6,729 recorded victims of sexual assault aged 0–14.¹⁷⁴ However, it is widely acknowledged that cases of child sexual abuse are chronically under-reported. Determining the scale of organised child sex offending is further complicated by Australian perpetrators abusing children overseas, as is the case with child sexual exploitation in travel and tourism.

Child sexual offenders are motivated by a diverse range of sexual attractions towards children and young people, spanning a broad continuum. This spectrum can range from offenders who view child exploitation material (CEM) online that has been produced by others, to offenders who interact with children and young people online for immediate sexual gratification, to persistent predators who groom children and young people online over time in order to lay the foundations for eventual sexual abuse in the physical world.

The range of contexts in which child sexual assault takes place varies. Through examination of subject matter literature, the Australian Institute of Family Studies has identified seven categories of child sexual assault perpetration. These are intrafamilial, adolescent (child-on-child), authority-figure (includes institutionalised abuse), stranger, online, Indigenous or other minority groups, and female perpetrators.¹⁷⁵

¹⁷⁴ Australian Bureau of Statistics 2013, 'Victims, sex and age group by selected offences—state and territory', in *Recorded crime victims, Australia, 4510.0*, ABS, Canberra, available at: <<http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4510.02012?OpenDocument>>.

¹⁷⁵ Australian Institute of Family Studies 2013, Summary for ANZPAA Child Protection Working Group feedback: AIFS and PwC gap analysis and recommendations to reduce child sex offending, AIFS, Canberra.

CASE STUDY

AUSTRALIAN FEDERAL POLICE OPERATION CONQUEROR

In January 2013, the Australian Federal Police identified persons of interest across Australia involved in a peer-to-peer file sharing network circulating CEM.

As a result of Operation Conqueror, to date a total of 40 search warrants have been executed and 25 arrests have been made. Offenders have been charged with offences that include producing, accessing, transmitting and making available CEM. It is estimated that, after further forensic analysis, millions of items of CEM will have been seized.¹

1 Australian Federal Police 2013, 'Further AFP arrests in child sexual exploitation cases', media release, 28 March 2013, <<http://www.afp.gov.au/media-centre/news/afp/2013/march/further-afp-arrests-in-child-sexual-exploitation-cases>>.

Technology is continuing to be a significant enabler for child sex offences, with new forms of exploitation emerging such as 'made-to-order' sexual abuse material, real-time sexual exploitation of children through pay-per-view services, and the emerging issue of 'sextortion'. Sextortion occurs when offenders coerce or deceive children and young people into providing sexually compromising imagery, which is then used as a tool to extort further CEM from victims.

Offenders are also increasingly exploiting the use of social media services and other online platforms (such as online gaming) to coerce victims to perform sexual acts in the 'virtual' environment online, and to groom children and young people for the purpose of conducting sexual acts. Given the growing importance of online activities in the lives of children and young people around the world (for educational, entertainment and social purposes), as well as the increasing uptake of the Internet in developing countries, the threat of child exploitation emanating from the online environment will continue to increase (see the case study above).

In addition, children and young people are adopting new technology earlier and at a greater rate, and thus unwittingly exposing themselves to online predators to an unprecedented degree. This includes child sexual exploitation for both private and commercial purposes.¹⁷⁶ Increased availability of high-speed Internet in the developing world is also expanding the sources of real-time CEM and increasing the number of children who can be victimised.

The online exploitation of children is a growing international concern, with advances in technology facilitating abuse. Darknets (and their online users) facilitating the exchange of CEM are concealed within freely available 'onion networks' such as The Onion Router (TOR), which consists of numerous relay servers and layers of encryption. Cheap prices for information and communication technology devices and easy Internet access permit sex offenders to have unprecedented access to materials and an online community to affirm their abusive and exploitative behaviour. Online services have also enabled offenders to share methodologies and experiences with like-minded individuals internationally, and to support the transnational exploitation of children. The ability to do this from a home environment also allows offenders to invest many hours in planning and undertaking activities to reduce the evidence of their offending online.

An emerging problem for Australia is the growth of youth gang and group culture that can involve the routine use of sexual violence against girls who associate with, or join, gangs. This behaviour is being seen in North America and the United Kingdom, where girls are often forced or coerced into participating in a range of sexual activities with male gang members, including sex with multiple partners at the same time or in quick succession.¹⁷⁷ This abuse can occur as part of initiation processes for male members, as displays of power, or for commercial exploitation.¹⁷⁸ In all of these situations, children are both the victims and the perpetrators of child sexual abuse.

Australia has in place an extensive legislative framework to prevent, investigate and prosecute all forms of child sexual exploitation, including offences that occur within Australia and those committed by Australian citizens and residents overseas. In April 2010, reforms were introduced to strengthen laws against child exploitation online and overseas. The reforms also reinforced the offences for using a carriage service (including the Internet) for child pornography or child abuse material.

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 more 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.

¹⁷⁶ United Nations Office on Drugs and Crime 2013, *UN crime body to combat online child abuse*, viewed 2 December 2014, <<http://www.unodc.org/unodc/en/frontpage/2013/September/un-crime-body-to-combatonline-child-abuse.html>>.

¹⁷⁷ Dorais, M & Corriveau, P 2009, *Gangs and girls: understanding juvenile prostitution*, McGill University Press, Montreal, pp. 29–30.

¹⁷⁸ Berelowitz, S, Firmin, C, Edwards, G & Gulyurtlu, S 2012, *I thought I was the only one. The only one in the world: the Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation in Gang and Groups (Interim Report)*, Office of the Children's Commissioner (UK), London, pp. 34–46.



THE OUTLOOK

What will the organised crime environment look like over the next two years?

The Australian serious and organised crime environment will continue to evolve over the next two years. What we are likely to see is the further integration of organised crime into legitimate markets, both to engage in criminal activities and to attempt to provide a façade of legitimacy for illicit operations. Organised crime will continue to adapt their criminal business model, to expand their use of flexible networked structures, to enhance their resilience and enable adaptive operations across international and domestic jurisdictions. They will continue to develop their capabilities, including adopting innovative information and communications technologies to support their activities. Australian law enforcement will increasingly look at the evolving challenges posed by the nexus between organised crime and terrorism over the next two years.

The use of professional facilitators to successfully exploit business structures on behalf of organised crime will remain a key problem, as lawyers, accountants and trust and company service providers are in large part not captured by Australia's Anti-Money Laundering and Counter Terrorism Financing regime. As a result, they do not have the same customer due diligence or 'suspicious matter' reporting obligations as financial institutions. This issue is under consideration as part of the statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, which is expected to culminate in a report and recommendations to the Australian Government in 2015. Professional facilitators will continue to perform an important role in the organised crime business model while they remain outside the Australian Anti-Money Laundering and Counter-Terrorism Financing regime.

The use of technology and the cyber environment by the majority of the community has opened new gateways for innovative methods of criminal targeting and compromise. The online culture of society today can provide organised crime with opportunities to engage in criminal activities anonymously and remotely. Our reliance on technology in everyday life means that the online environment, in particular, provides organised crime with a diverse pool of Australian victims. As organised crime becomes smarter at exploiting technology and members of the community increase their reliance on mobile devices, there is likely to be an increased susceptibility to compromise. Failure to install electronic security measures on mobile devices (such as phones and tablets) will remain an issue, as mobile devices are just as susceptible to attack as laptops and desktop computers.

The demand for certain illegal commodities, such as drugs, is ongoing and in the next two years will continue to dominate organised crime markets. Organised crime will continue to seek to satisfy this demand. The demand for methylamphetamine is currently being met by a combination of imported and domestically produced product, suggesting greater involvement by transnational serious and organised crime groups. The continuing high threat of the methylamphetamine market, and the effects it has on users, families, health services and the safety of the public, demonstrate the impact of organised crime in the community.

Where there are proceeds of crime, there will always be a need for money laundering. The banking and the alternative remittance sectors will continue to be major money laundering channels. The use of other methods of remittance, such as informal value transfer systems, to facilitate international money laundering is increasing. There are also indications that trade-based money laundering methodologies are being increasingly used as one component or stage of a money laundering process employed by global networks.

