



ORGANISED CRIME IN AUSTRALIA

2011

CONTENTS

INTRODUCTION	2
The contemporary face of organised crime	2
The impact of organised crime in Australia	3
UNDERSTANDING ORGANISED CRIME THROUGH RISK AND THREAT ASSESSMENTS	6
Market-based risk assessment	6
Threat and harm assessment	6
KEY FINDINGS REGARDING ENABLER ACTIVITIES	9
Identity crime	9
Money laundering	9
Violence	10
High tech crime	10
KEY FINDINGS REGARDING CRIME MARKETS	11
Illicit drug markets	11
Markets for other illicit commodities	14
Crimes in the mainstream economy	15
Crimes against the person	19
CONTEXT	20
How globalisation shapes organised crime in Australia	20
Organised criminal structures	28
Convergence with terrorism, corruption and political instability	33
Non-traditional organised crime markets	36
ENABLER ACTIVITIES	43
Identity crime	43
Money laundering	46
Violence	50
High tech crime	52
CRIME MARKETS	54
Illicit drug markets	54
Markets for other illicit commodities	73
Crimes in the mainstream economy	76
Crimes against the person	92
THE RESPONSE	94
Understanding changes in organised crime and crime markets	94
Collaboration	95
Increased public and industry awareness of key organised crime issues	97
Specialised law enforcement strategies	98
The ACC approach to combating organised crime	99
ABBREVIATIONS	100

INTRODUCTION



THE CONTEMPORARY FACE OF ORGANISED CRIME

Opportunities for organised crime today are unprecedented—increased globalisation, escalating cross-border movement of people, goods and money, emerging international markets and rapidly developing and converging technologies provide a fertile operating environment for organised crime.

The picture of organised crime built up over the past decade reveals a dynamic, ever-evolving transnational phenomenon of immense size.

Organised crime is sophisticated, resilient, highly diversified and pervasive. Current patterns of organised crime are more complex now than at any point in history.

Organised crime groups are entrepreneurial and unrestrained by legislation, borders, morality or technology. They are adaptable, innovative and fluid—infiltrating a wide range of industries and markets, well beyond areas generally considered vulnerable.


They are strategic and continually scan the marketplace for vulnerabilities, new opportunities and emerging technologies in order to make the greatest profit.

They are flexible about changing direction to achieve their goals. They adjust operations in response to law enforcement efforts to harden the environment. They collaborate for mutual benefit and can quickly disperse and regenerate in other markets if disrupted.

Organised crime operates within and alongside legitimate businesses, spanning multiple sectors to maximise return and minimise risk. Increasingly, organised crime uses logistics planning and aggressive marketing, buys in expertise and specialist facilitators and invests in research and development and risk mitigation strategies.

Complex networks which engage in illicit transactions stretch across continents to support activities that range from drug importation to identity fraud, cybercrime to high level offshore tax evasion, counterfeit goods to money laundering and even environmental crime.

To many, organised crime may seem like a distant threat, far removed from most people's lives. In reality, the social and economic harm that is caused through illicit drugs, financial crime and the associated violence and intimidation has a very real impact on the whole community.



Local level volume crime (crime other than serious and organised crime) understandably demands the greatest focus of state and territory police. However, the seriousness and pervasive impact of organised crime becomes clear when assessed against the threat and harm it causes. In this context organised crime is recognised as a national security issue in Australia.

THE IMPACT OF ORGANISED CRIME IN AUSTRALIA

Most organised criminal activities in Australia are focused on illicit drug markets, although organised crime groups also engage in a wide variety of associated criminal activity including tax evasion, money laundering, fraud, identity crime and high tech crime. The impact of organised crime in Australia is serious and far exceeds the direct harm caused by the specific offences.

In fact, the activities of high-threat serious and organised criminal enterprises result in significant harm to the Australian community. There are significant losses to the economy, including the redirection of resources that might otherwise be invested in legitimate business, reductions in tax revenue and increasing costs of law enforcement and regulation. The widespread impact extends to costs associated with longer-term health and social harm. The activities of organised criminal enterprises can also undermine public confidence in the integrity of key business sectors and government institutions.

The Australian Crime Commission (ACC) conservatively estimates that serious and organised crime costs Australia between 10 and 15 billion dollars every year.¹ Indirect costs such as those associated with illicit drug addiction, forced prostitution and community violence are also significant. Illicit drug abuse, for example, has an estimated social cost of over A\$8 billion annually.² There are also serious but non-quantifiable impacts including the collateral damage to family relationships, community functions and social cohesion, and potentially the loss of public confidence in the rule of law and the administration of justice.

“Most organised criminal activities in Australia are focused on illicit drug markets, although organised crime groups also engage in a wide variety of associated criminal activity including tax evasion, money laundering, fraud, identity crime and high tech crime”

- ¹ The ACC’s estimate of the cost of serious and organised crime is based on ACC intelligence and international research. Estimates of the cost of organised crime are produced by the United Nations Office on Drugs and Crime, the World Bank, Criminal Intelligence Service Canada, the Serious Organised Crime Agency, UK Department of Crime and Justice, and the US Department of Homeland Security. International estimates place the cost of organised crime, for most Western countries, between 1-2% of GDP.
- ² Collins, DJ and Lapsley, RM 2005, *National Drug Strategy*, Table 48. Australian Government, Canberra. Total social cost of drug abuse in 2004/05 was estimated at A\$8.2 billion. Alcohol and illicit drugs acting together added a further A\$1.1 billion.

THE IMPACT ON AUSTRALIAN SECTORS AND INFRASTRUCTURE

A consistent theme emerging from the external and domestic contexts within which organised crime operates in Australia is the diversity of the threat.

Organised crime directly affects many sectors and industries, including:

- > adult and general entertainment
- > banking and finance
- > chemicals and pharmaceuticals
- > education
- > firearms
- > import/export
- > information technology (IT)
- > insurance
- > luxury goods and apparel
- > maritime, aviation, road and rail transport
- > music, film and creative arts
- > private security
- > real estate
- > retail and wholesale business
- > social security
- > sport and fitness
- > stock exchange and private investment
- > superannuation
- > telecommunications
- > textiles
- > tobacco
- > wildlife and fisheries.

Accordingly, the domestic response includes, to a greater or lesser extent, law enforcement and public sector agencies of the Commonwealth, states and territories. These agencies have either a generic responsibility for enforcing the law, or are responsible for enforcement and regulation within relevant sectors and industries, or for policy development and implementation in the relevant areas. Additional stakeholders include departments and agencies that have access, both domestically and overseas, to information about the trends identified above.

Increasingly, effective responses to organised crime rely on cooperation from the private sector and the general public, both to report instances of suspected criminal activity and to collaborate in developing and implementing solutions (for example, through self-regulation or adopting business practices that protect the operating environment against organised crime).

The following chapters discuss specific threats and harm arising from a number of enabler activities and crime markets.



UNDERSTANDING ORGANISED CRIME THROUGH RISK AND THREAT ASSESSMENTS

6



MARKET-BASED RISK ASSESSMENT

Organised crime markets operate in the same way as markets for legitimate commodities—the primary motivator is financial gain and the markets are governed by demand, supply, price and the perceived quality of the goods that are (illegally) supplied.

In response, the ACC uses a market-based risk assessment approach that conforms to international risk assessment standards. This approach informs a comprehensive picture of serious and organised crime, its underlying methodologies and its impact on Australia. The ACC's risk assessment methodology involves a threat assessment and harms assessment process, with risk being a function of the assessed threat and harm levels:

$$\text{Risk} = \text{Threat (assessment of market dynamics)} \times \text{harm}$$

Threat and harm is assessed for each source of **risk**—that is various crime markets such as drugs, firearms, fraud and people trafficking, as well as enabler activities (often also criminal activities in their own right) such as money laundering and identity crime.

THREAT AND HARM ASSESSMENT

The **harm**, or consequences arising from those crime markets and enabler activities, is assessed from a political, economic and social perspective. The **threat**, or likelihood of those consequences, is assessed by considering market dynamics and the activities of market participants, taking into account the nature and effectiveness of existing controls (such as legislation or regulation) that impact on the market or enabler activity.

This market-based risk assessment underpins the ACC's *Organised Crime Threat Assessment*. The assessment provides contextualised information about the impact of serious and organised crime on the Australian community, market vulnerabilities and areas that would benefit from further intelligence or risk analysis.

This report is an unclassified version of the *Organised Crime Threat Assessment* that was delivered in June 2010 to the ACC Board and the ACC's partner law enforcement agencies.

The report outlines trends in the international environment, serious and organised crime³ activities in Australia and the resulting harms to the Australian community. It looks at supply and demand drivers and risks posed by a range of crime markets and key enabler activities.

The overall risk to Australia from organised crime is assessed as high.⁴ Relevant factors are:

- > The activities of organised crime groups breach existing controls in some markets and are sometimes deliberately focused in areas where controls are limited or difficult to establish and maintain.
- > Organised criminal activity is increasingly diverse and is evolving rapidly.
- > Organised crime has fatal consequences in some circumstances and some crime markets have significant adverse social (including health) consequences.
- > Organised crime generates billions of dollars of illicit proceeds and direct and indirect costs to governments, the private sector and the community of similar magnitude.
- > Organised crime requires a coordinated national (and, increasingly, transnational) response.

In particular, amphetamine-type stimulants, money laundering and identity crime pose a critical risk to the Australian community.

“In particular, amphetamine-type stimulants, money laundering and identity crime pose a critical risk to the Australian community”

3 The *Australian Crime Commission Act 2002* defines 'serious and organised crime' as an offence that involves two or more offenders, substantial planning and organisation and the use of sophisticated methods and techniques; which is committed in conjunction with other serious offences punishable by imprisonment for a period of three years or more. A broad range of serious offences is listed in the legislation including theft, fraud, tax evasion, money laundering, illegal drug dealings, extortion, bribery or corruption of an officer of the Commonwealth, an officer of a State or an officer of a Territory; perverting the course of justice, bankruptcy and company violations and cybercrime.

4 This assessment is based on the collective risk posed by the respective crime markets and enabler activities, but the level of risk has not been assessed relative to other national security risks.

While this report cannot provide the same level of detail as the classified version, it still clearly presents the disparate activities that make up the picture of organised crime in Australia. In doing so, it illustrates why an effective response to organised crime increasingly requires collaboration between many stakeholders—all levels of government, law enforcement agencies, public and private sector agencies, academic institutions and the public.

Given the highly diversified and ubiquitous nature of organised crime, there are clear benefits for a wide range of stakeholders better understanding the associated threats and risks. Informed, qualitative analysis supports improved decisions on how to most effectively use available resources to reduce the risks and combat the highest threats. The intention of this report is to inform public discussion, contribute to broader awareness and more informed decision-making, and provide a valuable baseline for future assessments.



THE NEXUS BETWEEN ORGANISED CRIME AND NATIONAL SECURITY

Australia's first National Security Statement released in December 2008 identified organised crime as a national security issue and highlighted it as '...a growing concern for Australia, one the Government is determined to combat'.

The Organised Crime Strategic Framework launched in November 2009 supports a more integrated and collaborative Commonwealth response to organised crime.

The ACC's *Organised Crime Threat Assessment* identifies the key organised crime risks so that Commonwealth agencies can combine their resources to respond to these risks.

The Commonwealth Organised Crime Response Plan aligns the resources of Commonwealth law enforcement agencies according to the priority risks identified in the *Organised Crime Threat Assessment*.

KEY FINDINGS REGARDING ENABLER ACTIVITIES

IDENTITY CRIME

- > Organised crime groups which engage in identity crime take advantage of weaknesses in identification and authentication processes.
- > Some organised crime syndicates have become professional identity crime 'specialists', with the single purpose of producing high-quality fraudulent identity documents.
- > Mail theft remains one of the enablers of identity crime.
- > Card skimming—the theft and use of identification data from financial transaction cards—is now considered a prominent feature of the identity crime market.
- > If chip and personal identification number (PIN) technology is more widely operational in Australia by 2013 it will reduce card skimming.
- > Identity crime is likely to increase in the future.



MONEY LAUNDERING

- > Legitimising the proceeds of crime and the instruments of crime (proceeds used to fund additional crime) is a crucial process for organised crime and therefore this activity is likely to continue to pose a critical risk.
- > Money laundering is an extremely diverse activity carried out in Australia at all levels of sophistication by most, if not all, organised crime groups, with or without the assistance of professional advisers.
- > Alternative remittance services continue to be widely used by organised crime groups.
- > International trade provides criminal syndicates with the opportunity to launder money.
- > Organised crime will consistently seek to exploit areas that receive less regulatory attention.

- > The response to money laundering underlines the benefits of broader partnerships between law enforcement and the public and private sectors to counter the diverse nature of the threat.

VIOLENCE

- > Violence between competing organised crime groups centres on matters of honour and reciprocal action, competition over territory or markets and enforcing illicit contracts and internal discipline.
- > Although violence may be used 'strategically', it is also frequently opportunistic or used without significant thought of gaining profit or advantage, sometimes without regard for consequences.
- > Increased violence by organised crime groups in some jurisdictions during 2009—including the violent incident at Sydney Airport and subsequent related attacks—appears to have reverted to more historical (lower) levels.
- > There is evidence that outlaw motorcycle gang members, regardless of ethnicity, are prepared to use violence to protect the membership and areas of influence of their particular chapter and group.

HIGH TECH CRIME⁵

- > Traditional organised crime groups use technology to communicate and to facilitate crimes such as drug trafficking, money laundering, extortion and fraud.
- > There is limited evidence that Australian-based organised crime groups are directly attacking computers and computer systems.
- > The principal threat to Australia from high tech crimes remains offshore.
- > Computers and the Internet are now linked to almost every facet of our lives and this electronic connectivity has created new vulnerabilities.
- > Criminal groups are moving away from traditional methods of infecting victims' computers through spam emails. Instead they are using what appear to be safe websites and environments which in fact contain embedded malware.
- > The risk posed by high tech crime is likely to increase in the short-to medium-term.

⁵ High tech crime is also referred to as cyber crime, but the former term has been retained for this assessment to maintain consistency with the classified version of the Organised Crime Threat Assessment.

KEY FINDINGS REGARDING CRIME MARKETS

ILLICIT DRUG MARKETS

COCAINE

- > Cocaine arrives in Australia from many intermediate locations, although the majority of cocaine detected at the Australian border continues to be directly imported from North and South America.
- > Networks involved in the production and international trafficking of cocaine are among the most sophisticated, profitable and powerful criminal networks in the world.
- > In terms of transnational supply routes, West Africa remains a problem.
- > In Australia, cocaine use and arrest rates are at historically high levels and law enforcement agencies have identified increasing availability of the drug throughout Australia.
- > There is increasing evidence that the harm from cocaine use is significant.
- > It is difficult to accurately assess and measure the cocaine market in Australia because of the relative lack of data compared with other illicit drug markets.
- > The risk posed by the cocaine market is likely to increase in the short- to medium-term.

METHYLAMPHETAMINE

- > The methylamphetamine market remains highly functional, resilient and entrenched.
- > Methylamphetamine use is no longer increasing, with primary national drug user surveys showing sustained decreases in reported use in recent years.
- > Methylamphetamine remains readily available, but some jurisdictions have identified volatility in the market.
- > Domestic production of methylamphetamine remains robust.





MDMA

- > Most MDMA consumed in Australia is imported.
- > Domestically, and in many countries around the world, the purity of tablets marketed as MDMA has been decreasing, with a range of other substances being pressed into tablets and sold as MDMA.
- > There are indications that MDMA is becoming increasingly available in Australia, but the market is re-developing slowly and high-quality MDMA remains largely unavailable.
- > Latent demand for high-quality MDMA remains strong.
- > The future trajectory of the MDMA market in Australia is difficult to assess.

DRUG ANALOGUES AND OTHER SYNTHETIC DRUGS⁶

- > Users throughout Australia are consuming a wide range of analogues and other synthetic drugs.
- > Many of these substances are sourced from online stores market themselves (incorrectly) as selling 'legal highs', legitimate fine chemical suppliers and sites selling 'research chemicals'.
- > The availability of these substances and the ease with which they can be purchased over the Internet has changed the traditional user-dealer relationship and resulted in a broad supply base.
- > The Internet also plays a significant role in diffusing information on drug analogues.
- > So-called 'legal highs' are marketed (incorrectly) as natural and legal and are perceived by users (in many instances, erroneously) to be less harmful than illicit drugs.
- > The speed with which the analogue market is evolving and the vast number of potentially active compounds will present law enforcement agencies and health authorities with unique challenges.

HEROIN

- > The demand and supply side of the Australian heroin market has remained generally stable over the past year, but some increases in heroin availability have been noted.
- > It is anticipated that the availability of heroin in Australia will continue to increase slowly, particularly in major capital cities.

⁶ Drugs with similar structures and effects to illegal recreational drugs, but different chemical and biological properties.

CANNABIS

- > The cultivation and distribution of cannabis in Australia is a large-scale, diverse and entrenched illicit market—resulting in cannabis remaining readily available.
- > Cannabis use has moderated in recent years, reflecting a trend also evident in other Western nations.
- > Despite the moderation in use, cannabis remains the most widely used illicit drug in Australia.
- > The cannabis market is highly decentralised and entrepreneurial with an array of individuals and groups operating at various levels of sophistication and capacity.
- > Despite the common perception that cannabis is relatively harmless, it does have a widespread impact on individuals and the general community.
- > The risk posed by the cannabis market is likely to remain stable over the next two years.

ILLICIT PHARMACEUTICALS

- > The illicit pharmaceutical market remains largely supplied by diversion from legitimate sources, with these drugs readily available on the illicit market from a diffuse network of suppliers, both illicit and legitimate.
- > The most recent National Drug Strategy Household Survey found that both recent use and use within a lifetime of painkillers/analgesics and tranquillisers/sleeping pills for non-medical purposes was higher than for most other illicit drugs.
- > The risk trajectory for this market is stable.

PERFORMANCE AND IMAGE ENHANCING DRUGS

- > There is widespread use of performance and image enhancing drugs.
- > Performance and image enhancing drugs are readily available.
- > The primary driver of this market in Australia is high demand as a consequence of the large potential user base, the variety of uses, ease of availability and potential profitability when on-sold.
- > The risk trajectory for this market is stable.





Gamma-hydroxybutyrate (GHB)

ANAESTHETICS

- > Gamma-hydroxybutyrate (GHB) is readily manufactured from its precursors, gamma-butyrolactone (GBL) and 1,4-butanediol (1,4-BD).
- > The GHB market has shown no signs of significant expansion in recent years and it is anticipated that the market will remain stable in the short- to medium-term.
- > The use of GHB has resulted in sporadic large-scale overdoses.
- > The use of ketamine remains confined to a small proportion of the community.
- > The low prevalence of ketamine use in Australia is in contrast to South-East Asia, where ketamine abuse has emerged as a significant problem.
- > Ketamine appears to be principally supplied through diversion from legitimate domestic sources.
- > The risk trajectory for these markets is stable.

TRYPTAMINES

- > The tryptamine market remains active in Australia.
- > Significant discussion is occurring in online forums on the use of lysergic acid diethylamide (LSD), psilocybin-containing mushrooms and dimethyltryptamine.
- > The tryptamine market is a niche market and its risk trajectory remains stable.

MARKETS FOR OTHER ILLICIT COMMODITIES

INTELLECTUAL PROPERTY CRIME—COUNTERFEIT GOODS

- > Counterfeit goods can either be goods that consumers know are counterfeit and are sold at a discounted price, or goods that are purchased at undiscounted prices in the belief they are genuine.
- > Goods in the latter category attract greater criminal involvement and may, depending on the type of good, pose the greater health and safety risk to consumers.
- > Australia has, by global standards, relatively low levels of intellectual property (IP) crime, but counterfeit goods are an expanding crime market in Australia.
- > Counterfeit goods seized in Australia include car parts, alcohol, cosmetics, laundry powder, batteries, textiles and clothing.



FIREARMS

- > In Australia there is continued demand for illicit firearms by organised crime groups, criminals generally and certain firearms enthusiasts.
- > Organised crime groups access illicit firearms from corrupt licensed dealers, criminal gangs and 'backyard' manufacturers.
- > Most illicit firearms seized appear to be commercially manufactured.
- > The risk trajectory for this market is stable.

CRIMES IN THE MAINSTREAM ECONOMY

INSURANCE FRAUD

- > Most insurance fraud relates to false or overvalued claims by individuals.
- > Improved information sharing within the insurance industry has helped detect organised criminal involvement in insurance fraud, particularly cross-company fraud.
- > Some crime groups are carrying out staged accidents and submitting multiple claims for the same loss.
- > Although the majority of organised criminal involvement in insurance fraud relates to motor vehicle insurance fraud, fraud related to marine craft and construction equipment is an emerging problem.
- > The risk posed by insurance fraud is likely to remain stable in the short- to medium-term.

SUPERANNUATION FRAUD

- > The structure and regulation of the superannuation industry in Australia restricts the ability of organised crime groups to target major superannuation funds.
- > In the case of self-managed superannuation funds the responsibility to detect or prevent fraud is placed on trustees who may be inexperienced, poorly trained and unqualified to perform the role and, sometimes, complicit in the fraud, making these funds particularly vulnerable to exploitation by negligent or disreputable trustees or professional service providers.
- > The number of self-managed funds is growing, creating a larger pool of potentially vulnerable funds.
- > Examples of organised criminal activity in the superannuation sector have been identified and there is potential for this activity to increase, despite the level of regulation and enforcement.





- > The majority of superannuation fraud relates to individuals accessing their own superannuation funds, but more organised early-release schemes continue to be promoted.
- > Identity theft and false identities remain the key enablers of superannuation fraud.
- > Although most superannuation fraud is committed by opportunistic individuals, evidence has emerged of groups specifically targeting superannuation holdings.
- > There is potential for the risk posed by superannuation fraud to increase in the short- to medium-term.

CARD FRAUD

- > Skimming devices continue to be attached to some automated teller machines (ATMs) in Australia, although the recent focus has been on skimming from electronic funds transfer at point of sale (EFTPOS) terminals.
- > Australian and transnational organised crime groups are known to be involved in card fraud.
- > If chip and personal identification number (PIN) technology proves effective, organised crime groups involved in skimming are likely to shift their operations to countries where this technology has not been implemented.
- > Card-not-present fraud⁷ increased in international markets when chip and PIN technology was implemented and this is expected to be mirrored in Australia.
- > The risk posed by card fraud is likely to increase over the next two years.

TELECOMMUNICATIONS FRAUD

- > The most common forms of telecommunications fraud involve using fictitious identities to acquire mobile and landline communication products and services.
- > Widespread uptake of 'mobile wallet' or 'e-purse' systems may provide opportunities for fraud.
- > The risk trajectory for this market is stable.

INVESTMENT FRAUD

- > Regulations and controls are extensive within the finance sector, but the diversity of the sector creates opportunities for criminals to generate large profits.

⁷ Card-not-present fraud refers to situations where the perpetrator deals with a merchant or service provider via mail, the Internet or telephone and obtains goods or a service fraudulently using false or stolen card details.

- > The use of company structures and legitimate business processes is crucial for many investment and financial services frauds.
- > There is limited evidence of organised criminal involvement in fraud and money laundering within the Australian financial securities industry.
- > A significant proportion of mortgage fraud originates through the mortgage broker network.
- > Ponzi schemes⁸ are a prominent form of fraudulent investment schemes.
- > The risk trajectory for this market is stable.

ADVANCE FEE FRAUD⁹

- > The extent of advance fee fraud in Australia has continually increased over the past five years.
- > Although advance fee fraud has traditionally been conducted by individuals in West Africa (particularly Nigeria), this type of fraud now emanates from a number of continents, including Europe and North America.
- > There is little evidence that Australian-based organised crime groups are involved in advance fee fraud, but isolated cases of individual involvement have been identified.

WELFARE FRAUD

- > Non-compliance represents the majority of Centrelink's overall customer debt, with fraud present in only a small percentage of cases.
- > The majority of welfare fraud is individual and opportunistic.
- > The cash economy is an ongoing area of risk.

REVENUE AND TAXATION FRAUD

- > Intelligence suggests that organised crime groups are having an increasing impact on the taxation system by exploiting a range of areas such as refund fraud, illicit tobacco and offshore tax arrangements to conceal income or falsify deductions.
- > Organised crime groups have also been identified engaging in excise fraud.

⁸ A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organisers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, the fraudsters focus on attracting new money to make promised payments to earlier-stage investors and to use for personal expenses, instead of engaging in any legitimate investment activity. With little or no legitimate earning, the schemes require a consistent flow of money from new investors to continue. Ponzi schemes tend to collapse when it becomes difficult to recruit new investors or when a large number of investors ask to cash out.

⁹ Advance fee fraud is defined as any fraud requiring a victim to make payment/s in advance of the promised receipt of a large monetary or other material benefit.





tobacco leaf

- > Organised crime groups are increasingly using a sophisticated network of businesses, proprietary companies, partnerships and/or trusts for the purpose of facilitating criminal activities and laundering significant amounts of cash.
- > As at 31 December 2010, the multi-agency Project Wickenby has raised additional tax assessments totalling \$988.93 million, recouped \$238.25 million in tax, achieved a compliance dividend of \$301.70 million and collected \$2.1 million in other moneys—resulting in a total collection of \$542.05 million.
- > The agencies involved in Project Wickenby are also deterring people who were likely to evade tax.
- > The risk trajectory for this market is stable.

ILLEGAL TOBACCO

- > Organised crime networks have been linked to the importation of counterfeit cigarettes and loose tobacco.
- > Significant government revenue is avoided through the activities of groups involved in illicit tobacco importation and illicit growing, curing, manufacture and sale of tobacco products.
- > The successful interdiction of illicit tobacco products at the border, the high illicit profits and increases in the excise duty on tobacco products are likely to increasingly attract organised crime groups to the illicit tobacco market.

HEALTH FRAUD

- > Criminal behaviour in the health sector is largely high-volume, low-level non-compliance and fraud.
- > Fraud represents only a small proportion of total non-compliance.
- > Health fraud generally involves professionals working within the industry and individuals external to the industry.
- > There are few major cases of fraud against Medicare Australia and the Pharmaceutical Benefits Scheme (PBS).
- > International trends suggest more organised criminal activity in the health sector is probable in the future.

CRIMES AGAINST THE PERSON

PEOPLE TRAFFICKING

- > In Australia, the majority of victims identified by authorities have been women working in the sex industry, however authorities are becoming increasingly aware of people who have been trafficked for exploitation in other industry sectors.
- > The hospitality, agricultural, construction, domestic services, recreation and sex industries are key targets of exploitation by people traffickers.
- > The risk trajectory for this market is stable.

IRREGULAR MARITIME ARRIVALS

- > Displaced persons perceive Australia to be an attractive destination country because of its geographic location and positive economic, political and social environment.
- > Since September 2008, there has been a significant increase in irregular maritime arrivals.
- > Reporting indicates a continued threat to Australia from organised people smuggling and, to a lesser extent, independent ventures.
- > The risk posed by this market is likely to increase in the short- to medium-term.



CONTEXT



HOW GLOBALISATION SHAPES ORGANISED CRIME IN AUSTRALIA

INTERNATIONAL TRENDS

Organised crime has moved well beyond a simple law and order problem within the remit of an individual agency, jurisdiction or country.

Organised crime today is a transnational, highly capable and multi-dimensional threat, inextricably linked to global economic activity and national security issues.

Transnational crime and corruption threaten global interests by undermining security and stability, the rule of law and legitimate business activities.

Although the effects of organised criminal activities are felt locally in many ways by numerous businesses, communities and individuals, the harms generated resonate internationally.

ORGANISED CRIME GOES GLOBAL

The United Nations (UN) Office on Drugs and Crime stated in its June 2010 transnational organised crime threat assessment that:

Organized crime has diversified, gone global and reached macro-economic proportions: illicit goods are sourced from one continent, trafficked across another, and marketed in a third... In terms of global reach, penetration and impact, organized crime has become a threat affecting all states.

In his preface to this report, former Executive Director, Antonio Maria Costa, commented that:

...since crime has gone global, purely national responses are inadequate [as] they displace the problem from one country to another.¹⁰

¹⁰ *The Globalization of Crime: A Transnational Organized Crime Assessment*, UN Office on Drugs and Crime, Vienna, June 2010.

INCREASED MOVEMENT, COMMUNICATION AND TRADE

Just as legal businesses now operate in a borderless world, organised crime groups have harnessed advances in travel, communications, finance, technology and the Internet. They move illicit goods with impunity around the globe through established routes and networks. The networks have instant access to domestic and international markets and can swiftly switch countries and deal in multiple commodities. Australia and the Pacific region can be targeted from any location globally.

INCREASED REACH INTO LEGITIMATE BUSINESS

Overseas experience indicates that transnational crime groups increasingly operate within the legitimate economy in sectors such as banking and international finance, high technology, pharmaceuticals, shipping and manufacturing—also areas of potential concern within Australia. In some cases, the activities of organised criminal networks are almost indistinguishable from legitimate corporations. Unlike some legitimate enterprises, however, organised crime networks have prospered in times of economic recession or economic growth due to their flexibility and capacity to exploit changing market vulnerabilities.

ORGANISED CRIME GROUPS EXPLOIT ECONOMIC ADVERSITY

There is little evidence that organised crime groups suffered significantly during the global economic crisis—indeed, there is convincing evidence that they have benefited considerably from the economic downturn by infiltrating legitimate business sectors.

For example, the Yakuza allegedly increased its presence in the Japanese consumer finance sector by providing finance (at a cost) when lending institutions became financially unviable after the Japanese Government tightened lending restrictions. Similarly, during the 1997 Asian financial crisis, cashed-up Chinese organised crime groups made significant purchases in the Hong Kong property market.

It is now possible for billions of dollars to be relocated around the globe with low visibility and minimal risk. Criminal proceeds derived in one jurisdiction can be laundered in numerous locations around the world.

AMERICAN BANK LAUNDERS MEXICAN ILLICIT DRUG PROCEEDS

In March 2010, a United States (US) bank paid US\$160 billion in restitution and penalties to settle a federal investigation into the laundering of illicit drug profits from Mexico through the bank's offices and Mexican foreign exchange houses. Up to US\$110 billion was reportedly laundered through the bank.

COUNTERFEIT GOODS

Globalisation provides opportunities for organised crime to exploit greater financial integration and trade. Trade in counterfeit goods is expanding globally and is estimated to have increased eight times faster than legitimate trade since the early 1990s.

While counterfeit goods are generally associated with the luxury goods market, this crime market also extends into many other sectors, with far reaching effects for those wholly unconnected with it. For example, in 2008, global seizures of counterfeit pharmaceuticals increased sevenfold. The harm posed by this activity ranges from circumvention of patents to sale of preparations containing limited or no active ingredients. In some cases, this can have lethal consequences for people using the sub-standard medication, or can permit the targeted organism to mutate and become resistant to genuine pharmaceuticals. There are also potentially lethal consequences from counterfeit parts for motor vehicles and aircraft.

Counterfeit goods are estimated to account for between five and seven per cent of overall world trade and to be worth A\$400–600 billion annually.¹¹

SOCIAL ASPECTS

There are also social dimensions to globalisation, such as the increasing number of people seeking to move from poor to wealthier countries. Mass migrations may be exacerbated by climatic changes diminishing water and food producing capacities in some regions. African countries are likely to fare the worst in terms of long-term poverty and the poorer the country the more likely that organised crime groups, extremism and corruption will take hold. Moreover, particular crime groups are taking advantage of ethnic diasporas¹² to expand their influence and access to illicit commodities and trafficking routes. Examples are West African, Latin American and Middle Eastern groups.

11 Treverton, GF, Matthies, C, Cunningham, KJ, Goulka, J, Ridgeway, C & Wong, A 2009, *Film piracy, organized crime, and terrorism*, RAND Corporation; Yar, M, 2005; A deadly faith In fakes: trademark theft and the global trade in counterfeit automotive components, *Internet Journal of Criminology* 2005, p.2, available at <www.internetjournalofcriminology.com>

12 Dispersed groups of persons throughout the world who share a common ethnic, cultural, racial, religious or political background.

Organised crime reaches into all levels of society. The global economic crisis showcased how organised crime groups are not limited to traditional stereotypes. Cynical, criminally-minded entrepreneurs and advisers from the 'top end of town' caused massive harm to economies, homeowners, consumers and investors. In the US, for example, Bernard Madoff was responsible for a US\$65 billion investment fraud and Florida lawyer Scott Rothstein for a similar US\$1 billion Ponzi scheme. Madoff was sentenced to 150 years imprisonment, reflecting the gravity of his crime.

SHIFT IN ECONOMIC POWER

The global economic crisis, and the resultant focus on debt levels and flaws in the regulatory framework in the US and Europe, has fuelled discussions about a gradual shift in global economic power to the Asia-Pacific region, particularly the People's Republic of China (PRC) and India. It is possible that Russia, Brazil, Korea and Indonesia will also emerge (or re-emerge) as significant powers in decades to come. Notably, several of these countries are already focal points for transnational organised crime, either as source countries for illicit commodities or as locations where trafficking routes for illicit commodities intersect, known as transshipment nodes.

ADVANCES IN INFRASTRUCTURE AND TECHNOLOGY

In South-East Asia, infrastructure improvements (including international highways and trade centres) and free trade agreements already assist the rapid movement of people and commodities, providing opportunities for organised crime groups.

Technological advances also permit organised crime groups to use sophisticated techniques, for example in relation to advance fee fraud, card fraud and skimming¹³ and 'virtual worlds'. Virtual worlds in some cases encompass a real cash economy and real money transactions, estimated at up to US\$2 billion a year, and have been linked to intellectual property crime and money laundering.

DOMESTIC IMPACT

Features of contemporary Australian society reflect those aspects of globalisation that create opportunities for organised crime. Australia's multicultural society enables criminally minded people from organised crime groups which contain persons from a variety of social and ethnic backgrounds to operate within local communities, particularly in the larger cities.



¹³ Card skimming is the illegal copying of information from the magnetic strip of a credit or debit card.



ECONOMIC AND FINANCIAL FACTORS

Australia enjoys a relatively high standard of living, a robust and well-regulated banking and financial system and a social security infrastructure that supports citizens and permanent residents in defined circumstances.

Levels of international trade into and out of Australia are sufficient to disguise organised crime-related payments. In addition to normal banking processes, alternative remittance services are available to organised crime groups. These groups exploit the Australian cash or shadow economy to fund drug purchases, conceal the proceeds of crime and meet general living expenses. The cash economy is also exploited by crime groups in markets such as private security, illegal immigration and sexual servitude.

The increasing scale of Australia's political and trade ties with some of the world's major developing economies, and our proximity to Asian economies and capital markets, presents opportunities for transnational and domestic criminal networks to create and develop illicit markets. While transnational criminal enterprises are likely to focus on countries experiencing unstable political circumstances with weakened governance controls, Australia is a lucrative market for illicit commodities and is not exempt from their attention.

GEOGRAPHICAL FACTORS

Australia's geography provides some insulation against organised crime, as various types of illicit commodities have to be imported. However, there is also a downside to geographic isolation. It means we depend on high volumes of legitimate sea and air freight within which illicit commodities can be concealed.

The Australian Customs and Border Protection Service (Customs and Border Protection) estimates that trade volumes and numbers of international visitors are likely to increase significantly by 2015. For example, between 2007 and 2015, import sea containers are estimated to increase from 2.2 million to 3.7 million, air cargo consignments from 10.3 million to 17.5 million, postal articles from 150 million to 220 million, passengers from 23.544 million to 34.152 million and arriving ships from 12 824 to 22 885.¹⁴

Australia's long and vulnerable coastline also provides opportunities for illicit goods to come into the country via small vessels or light aircraft.

In addition, transnational criminal groups rapidly adopt information and communication technologies, enabling them to operate in a borderless world—cherry picking opportunities across jurisdictions and exploiting large numbers of people regardless of location—further reducing the advantages of Australia's isolation.

14 Customs and Border Protection, *Strategic Outlook 2015*.

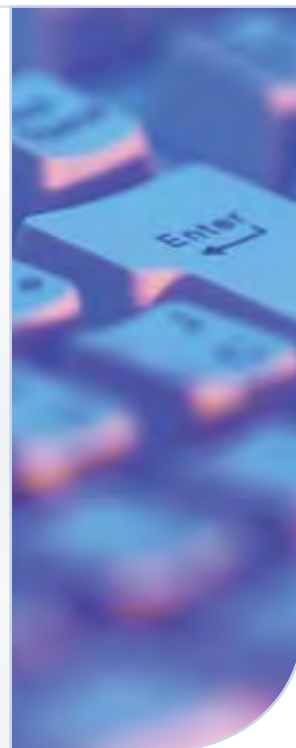
TECHNOLOGICAL FACTORS

With our major cities separated by significant distances and our widely dispersed rural population, Australia needs effective long-distance telecommunications networks and we rely heavily on computers and related information technology. Australia's telecommunications system is well developed and reliable by world standards. We have one of the highest global take-up rates of new technology and a well-educated population that is a ready market for many types of technology. This provides exploitable opportunities for organised crime and helps transnational groups operate effectively in Australia and maintain contact with group members overseas.

The rapid take-up of technology and the development of broadband Internet has the potential to generate an increase in the incidence of high tech crime in Australia. This encompasses both traditional criminal activity using technology as well as crime directed at information and communication technologies. Traditional criminal activity uses technology to facilitate money laundering, identity theft, online child exploitation, fraud, unsolicited bulk email ('spam') and copyright offences. The convergence of mobile phone and Internet applications gives criminals an increasing array of possible targets and capabilities. Regardless of the method and devices employed, a serious denial of service attack on computer systems that control a key piece of infrastructure used in the banking and finance, light and power or telecommunications sectors could have devastating consequences.

RESPONDING TO HIGH TECH CRIME

Countering computer-based and technology-based crime has become a key priority for the Australian, state and territory governments in terms of national security and law enforcement. A number of agencies are involved in combating high tech crime, including the Attorney-General's Department, the Australian Communications and Media Authority, the Australian Federal Police and the Defence Signals Directorate. The newly established Computer Emergency Response Team, or CERT Australia, within the Attorney-General's Department, will be the central source of cyber security information for the Australian community and the key point of contact for the Australian business community and Australia's international cyber security counterparts. CERT Australia, together with other operational Australian Government agencies, works closely with the Cyber Security Operations Centre within the Defence Signals Directorate, which advises the Australian Government of cyber security threats and enhances the ability to coordinate an operational response to major cyber security incidents.





IDENTITY CRIME

Australia's high take-up of communications technology also facilitates identity crime. This global phenomenon has become a hallmark of serious and organised crime and has significant social and financial ramifications. The large volume of personal information on social networking sites such as Facebook provides an opportunity for organised crime groups to obtain data and create identification documents for criminal purposes. Criminals have access to a range of options through information and communications technology systems to obtain or produce high-quality and low-cost fraudulent identity documents.

ONLINE SALES

With the ever expanding variety of goods for sale online, the Internet has created a global market for illicit commodities. Examples in Australia include counterfeit goods, drug analogues, cannabis seeds, performance and image enhancing drugs, precursor chemicals and the illicit trade in flora and fauna.

CARD FRAUD

Similarly, by exploiting the Internet, organised crime groups involved in card fraud establish geographically dispersed criminal networks that can quickly execute fraudulent transactions in multiple locations remote from where the skimming originally occurs. The Internet is used to transmit skimmed data, to seek technical or specific product expertise and to buy specialised equipment such as card readers. Australia has been targeted by transnational card fraud networks.

Credit card and debit card fraud in Australia has continued to increase substantially over the past three years. There were 63 894 fraudulent debit card transactions to a total value of A\$24 471 348 during the year ended 31 December 2009, compared with 34 318 fraudulent transactions to a total value of A\$14 393 443 during the year ended 31 December 2006. For the same years, there was an increase in credit/charge card fraud from 241,063 transactions totalling A\$85 215 615 in 2006 to 593 819 transactions totalling A\$145 854 208 in 2009.¹⁵ The greatest loss from card fraud is generated by card-not-present fraud, followed by counterfeit or altered cards, lost or stolen credit cards and fraudulent applications.

¹⁵ Australian Payments Clearing Association, 2010, *Fraud Perpetrated on Australian Issued Payment Instruments 1 January 2009 – 31 December 2009*, <www.apca.com.au> viewed 27 January 2011.

Card-not-present fraud increased by approximately 25 per cent for the 12 months to June 2009. Card fraud is estimated to have cost Australia A\$147 million during 2009, slightly more than the A\$144.7 million cost in 2008. Significantly, card-not-present fraud increased in international markets when chip and PIN technology was implemented to reduce card skimming. This is expected to be mirrored in Australia after the universal implementation of chip and PIN technology by 2013.

ADVANCE FEE FRAUD

Losses associated with advance fee fraud continue to increase, again facilitated by the increasingly sophisticated exploitation of electronic communications by organised crime groups. Advance fee fraud is one component of mass marketed fraud that has grown exponentially as a result of increased computer ownership, Internet use and cheap telephony. Advance fee frauds are committed using a wide range of methods, including postal mail, facsimile, telephone, email and Internet sites (including 'chat rooms', dating websites, Internet auction websites, social and business networking sites and Internet gaming).

There has been a recent increase in advance fee fraud through short message service (SMS) text messaging, which offers more efficient transmission of information than the traditional use of mail. The extensive use of digital communications technologies allows cost-effective and instantaneous worldwide contact with victims, while disguising the true locations and identities of perpetrators. The capacity of money transfer services to send and receive funds anywhere in the world has also furthered the expansion of advance fee fraud.

CHILD SEX OFFENCES

Advances in technology, and the expansion of the Internet, have also led to an increase in 'strategic child sex offending'. Offenders have become increasingly sophisticated in their networking activities and more able to access information to facilitate their offending. This is a critical concern in attempts to combat child sex offences. The UN Office on Drugs and Crime noted in 2010 that the growth of the Internet has reduced the risk of detection for people responsible for the production and acquisition of child pornography and has created the potential for increased demand, setting the scene for a growth in this form of criminality.¹⁶

¹⁶ UN Office on Drugs and Crime 2010, *Globalization of Crime*, pp 13, 212 and 213.





SUMMARY

The impacts of globalisation are an inherent part of life in Australia. However, with the benefits come opportunities for organised crime groups and challenges for law enforcement and regulatory agencies.

Globalisation has broadened the reach of organised crime to the point where aspects touch almost everyone's life in some way. This, in turn, broadens the range of agencies that are stakeholders in preventing and detecting organised criminal activity, including government and quasi-government agencies, departments and private sector entities, communities and individuals.

ORGANISED CRIMINAL STRUCTURES

The power, networking ability and opportunism of sophisticated transnational criminal groups means they now operate at an unprecedented level around the world. Some groups wield immense power. The reach and influence of leading members of the larger transnational crime groups stretches far beyond their home country. For example, Mexican drug cartels now have a foothold on most continents and profits that rival the GDP of some of the world's smaller nations.

In Australia, organised crime involves a highly interconnected milieu of criminally minded groups and individuals, which come together as opportunities arise. Organised crime groups in this country vary significantly in sophistication, structure and modus operandi, dependant on their perceptions of the opportunities and threats that exist at that time. The organisational structures adopted by criminal networks are heavily influenced by their perceived opportunities and threats. Rapidly evolving and temporary criminal structures and capabilities create problems for government and law enforcement agencies in identifying and 'triaging' targets and aligning operational and legislative responses.

Organised criminal groups and networks operating in Australia, whether transnational or domestic, can be formidable in terms of their capabilities, resources and resilience. They exploit existing opportunities and create new ones. Many rely heavily on enablers including identity crime, communications technologies and access to professional expertise, while some benefit from access to corrupt officials.

Organised criminal groups are innovative and protect themselves through counter-intelligence/counter-surveillance and by working within closed networks of trust. Some groups continue to rely on violence, intimidation and extortion, which remain fundamental to organised criminal operations. This can generate fear in legitimate businesses trying to operate in the same market. Combined with the fact that organised crime groups operate outside normal moral and legal frameworks, this gives them a significant competitive advantage in these markets.

In Australia, hierarchical groups that are defined by membership criteria are less prevalent than loose networks of individuals that come together as opportunities arise. This shift in the structure of organised crime groups is also increasingly apparent in Europe. As a result, the European Union has shifted its conceptual focus from targeting organised crime (based primarily on identifying who is committing the crime) to serious crime (that is, the effect of the crimes themselves, such as drug trafficking or violence, and the broader impact on the community of the respective crime markets). In Australia, the distinction is exemplified by the high-end criminal groups involved in heroin or cocaine importations, for example, compared with those involved in the drug analogue market, which poses a significant threat but which currently has limited organised criminal involvement. Both types of activity must be disrupted, because of the magnitude of the risk, rather than because of the characteristics of the offending groups and individuals.

TRADITIONAL HIERARCHICAL STRUCTURES

Most high-threat criminal enterprises actively seek to insulate their criminal activities by intermingling legitimate and illegal interests. Historical organised crime structures relied on hierarchical control within tight ethnic or cultural security arrangements. They often used a corporate business model similar to those of the legitimate business sector, involving strategic planning, recruitment of specialised expertise, internal security and risk management. Internationally, traditional hierarchies, typified by the Sicilian Mafia or the Yakuza in Japan, remain resilient and effective in their specific markets. However, other transnational criminal enterprises have varied traditional hierarchical command and control structures by moving to adaptable and more flexible structures, including in some cases franchise models.¹⁷

Traditional hierarchical organised criminal groups are increasingly responding to changing market dynamics and law enforcement interdiction. They are offsetting the disadvantages inherent in rigid and sometimes brittle hierarchical command structures through networked or hybrid structures and innovative use of information and communications technologies.

Increasing collaboration between different transnational criminal networks creates more flexibility to exploit criminal opportunities and markets around the world.

Transnational crime networks supply illicit drugs to Australia including heroin, cocaine, 3,4-methylenedioxymethamphetamine (MDMA, also known as ecstasy), some forms of methylamphetamine and precursor chemicals. In some cases the networks have a local footprint, but in other cases they remain offshore and collaborate with local crime networks to arrange specific or periodic importations.

¹⁷ See Glenny, M 2007, *McMafia: a journey through the global criminal underworld*, New York.

Transnational networks also have a presence in other Australian crime markets. For example, the high tech crime threat to Australia mainly comes from offshore. This largely arises from temporary and opportunistic networks that specialise in technology-based offences involving data compromise, identity theft and compromising websites. Moreover, transnational money laundering syndicates have a tangible presence in the Australian market.

Foreign-based organised crime groups involved in advance fee fraud are also increasing in size, sophistication and organisation. International groups are more often combining advance fee fraud with other offences such as identity crime, trading of counterfeit goods and, in some cases, drug trafficking. Organised crime groups involved in advance fee fraud exploit the multi-jurisdictional nature of their crimes, which poses particular challenges for law enforcement to identify and subsequently disrupt the activity.

Of necessity, people traffickers and networks that transport irregular maritime arrivals¹⁸ to Australia operate transnationally. Payments to crime networks by or on behalf of irregular maritime arrivals are almost exclusively made offshore and the majority of the criminal activity occurs outside Australia.

Transnational networked criminal enterprises pose a jurisdictional and logistical challenge to law enforcement and regulatory agencies and present different but equally important challenges to law makers and policy agencies. The best defence against transnational crime is multi-national and multi-agency investigations designed to disrupt the international networks at key hubs where trafficking routes intersect and where they may be vulnerable. Timely exchange of intelligence with affected countries and agencies is also crucial.

NETWORKED STRUCTURES

Transnational groups active in Australia are increasingly characterised by networked or hybrid hierarchical structures. This helps them insulate command levels, rapidly repair damage and adapt methodologies. Investigations have revealed the variety and fluidity of relationships between organised criminal groups across jurisdictions and their increasing interaction across social and cultural boundaries. In such cases, the relationships between the principals are based primarily on available resources rather than traditional ethnic or cultural trust structures. These groups have demonstrated an ability to operate in both illegitimate and legitimate business sectors.

¹⁸ Irregular Maritime Arrivals are people who arrive without authority by boat in Australia, either on the mainland or at an excised offshore place.

CASE STUDY: NETWORKED AND HYBRID CRIMINAL STRUCTURES

Criminal syndicates importing powder MDMA from Europe to Australia have adopted a networked or hybrid hierarchical structure. Networks of established criminal syndicates operating in Australia are well resourced and highly resilient. Several senior members have been under long-term investigation by law enforcement agencies. These syndicates have enlisted the services of previously unrelated, established organised criminal networks to manage each aspect of their drug importation and distribution operations.



They forge robust links between the membership of key networks and form temporary command hierarchies. To increase operational security and protect key players, agreed network members are entrusted to recruit people to move imported MDMA from vessels through relevant Australian ports to safe-houses, where local criminal groups handle domestic distribution.

These networks have included persons of Balkan background, members of outlaw motor cycle gangs and people with legitimate access to Australian ports. Networked criminal activity for the importation and distribution of MDMA has occurred across several European countries and New South Wales, Victoria and Western Australia.

There is also recent evidence that a number of transnational groups are now willing to temporarily collaborate with domestic criminal groups with whom they have had little or no previous association, where there is a mutual benefit. The association mirrors franchise arrangements in legitimate business and may be for one or several major criminal transactions (such as drug importations).

In layers beneath the most sophisticated organised crime groups are large numbers of groups that also operate like legitimate business, creating and taking advantage of market opportunities, exploiting vulnerabilities and relying on networks of trusted contacts who can facilitate their criminal activity. In many cases, Australian organised crime groups are simultaneously involved in several crime markets. Key organised crime identities operate as hubs or nodes to link a series of criminal groups and in some cases perform the role of a consultant and facilitator. Often, members of organised crime groups are relatively unsophisticated in their activities, but rely on their connections to key criminal associates to achieve their aims.

NET-CENTRIC STRUCTURES

Transnational networks active in Australia increasingly use a wide variety of Internet-based communications to link disparate criminal elements sharing specific criminal objectives, financial interests, available skills and advanced methodologies.

Groups operating in Australia have used information technologies and communications devices to build resilience against law enforcement. For example, some groups use portable communications devices to generate secure encrypted communications.

In other crime markets, technology is reducing the need for organised criminal involvement. For example, people shop around the Internet for information on new drugs and supplies of various illicit drugs and precursor chemicals. Moreover, the Internet facilitates identity crime, fraud, high tech crime, money laundering and a range of other offending. Technology has opened up new crime markets, including to people not traditionally involved in serious and organised crime—criminal activities with national and international reach can now be coordinated from a computer in a suburban lounge room.

RESILIENT CRIMINAL NETWORKS

Australian criminal groups have evolved over the past 50 years in line with all the above factors. The most resilient groups are those which have:

- > exploited competitive advantages in their particular illicit markets
- > recognised and taken advantage of opportunities in a number of crime markets (often as a result of identifying changes in demand)
- > gained access to people with particular criminal expertise or knowledge and skill sets that can be exploited for criminal purposes
- > developed the flexibility to collaborate with other crime groups for particular transactions
- > exploited knowledge of law enforcement methodologies to insulate themselves against detection and disruption.



CONVERGENCE WITH TERRORISM, CORRUPTION AND POLITICAL INSTABILITY

The activities of transnational organised crime groups and some terrorist groups converge where their illicit networks intersect. Failed, failing and rogue states provide safe havens for organised crime, impetus for the production and distribution of illicit commodities and an environment where organised criminal activity and the interests of extremist or terrorist groups can converge.

Rapid population growth and increased urbanisation in developing countries are encouraging an increase in criminality and creating a breeding ground for political extremism. Failed, failing and rogue states, some of which are Australia's regional neighbours, now outnumber stable states by roughly two to one. As well as providing a base for both organised crime and terrorist groups, these states have in some cases been directly implicated in drug and arms trafficking. West and East African states with high levels of corruption and limited law enforcement capabilities feature prominently in this category.¹⁹

FAILED STATES INDEX 2010

A total of 177 countries were measured in the Failed States Index 2010. Professor Andy Hughes of the Centre for Transnational Crime Prevention, University of Wollongong, noted in October 2010 that eight of 15 West African countries measured were in the bottom 60 countries on the index.

Four of the eight countries in Australasia-South West Pacific measured were also in the bottom 60 countries, and three of those countries are deteriorating.

He also noted that nearly all fragile states identified in 1980 are still fragile today and that World Bank analysts predict that a fragile state is likely to retain that status for at least 56 years.



The world is now moving towards a multi-polar political model of global power and there has been a shift towards the Asia-Pacific region as the power base. At the same time, non-state entities, including multinational corporations, pressure groups, the larger organised crime groups and terrorist or insurgency groups, are projecting power and influence that at times demand attention on a global scale. The Italian N'drangheta, which has an Australian footprint, has an estimated annual turnover of A\$60 billion. The combined annual turnover of the Mexican drug cartels, which are increasingly exporting cocaine to Australia, is estimated to exceed \$10 billion—placing them on the same revenue footing as some Fortune 500 companies.

¹⁹ Foreign Policy magazine and *The Fund for Peace*, 2010, *The Failed States Index 2010*, Washington DC; Huria, S, 2008, *Failing and Failed States: The Global Discourse*, Institute of Peace and Conflict Studies, New Delhi.

A number of nations that are prominent sources and transshipment hubs for illicit commodities are extending their influence around the globe by establishing closer trade links with Africa and South America. Organised crime groups from those nations are following closely behind legitimate businesses and Africa and South America now feature prominently in international drug trafficking routes.

The confluence of organised crime, terrorism and corruption is an enabling environment for moving and exchanging drugs, arms, people, stolen or pirated goods and for funding criminal and extremist activities. Often the same routes, networks and methodologies are used for these activities.

The convergence is of most concern when it is married with the increasingly blurred distinction between the politically-motivated activity of some terrorist groups and the criminal activities that fund them. Elements within Hizballah, Al-Qa'ida/the Taliban, Hamas, the former Liberation Tigers of Tamil Eelam and the Kurdistan Workers' Party operate or have operated criminal enterprises for profit or to advance their terrorist agenda. Other examples of such convergence have been noted by the UN Office on Drugs and Crime in Europe, South America and South-East Asia.

The Madrid train bombings in 2004 were committed by a group comprising members of a terrorist cell and an organised crime group, with much of the funding and logistics provided from proceeds of drug trafficking. The Taliban-led insurgency in Afghanistan has been financed in part by the drug economy, with the Taliban providing protection for drug traffickers in the districts they control.



The Madrid train bombings in 2004 - AAP

Hizballah and Hamas now have influence and access to illicit drugs in Mexico, Africa and South America. The Liberation Tigers of Tamil Eelam, before its demise, accessed funds from supporters in Australia, Canada, the US, Scandinavia, Western Europe and South-East Asia. The Liberation Tigers of Tamil Eelam was also implicated in trafficking arms, people and drugs. The Revolutionary Armed Forces of Colombia receives significant funding from cocaine production and trafficking and there are reports that it controls up to 70 per cent of Colombian cocaine production. The US Drug Enforcement Administration said in August 2010 that the Revolutionary Armed Forces of Colombia is responsible for the production of more than half of the world's supply of cocaine and nearly two-thirds of the cocaine imported into the US.

Organised crime is taking advantage of political instability in Myanmar, Afghanistan, Mexico and Iran. In the last three countries and in Colombia, the military as well as law enforcement are responding by targeting organised crime groups, with varying degrees of success.

IS THERE DOMESTIC CONVERGENCE?

States that face the greatest problems from organised crime groups generally exhibit a mixture of political instability and corruption that facilitates organised crime. Conversely, Australia has stable democratic political institutions, an independent judiciary and a broadly based respect for the rule of law.

Australia does not have a history of major political extremism. Rather, successive governments have reacted robustly against terrorism here and abroad. Since the late 1970s there have been instances of terrorism in Australia. Prosecutions indicate a level of support for Middle Eastern and Asian terrorist groups and their offshoots in this country. Eighteen terrorist organisations are currently 'listed' pursuant to the *Security Legislation Amendment (Terrorism) Act 2002*. To date there has been very little local evidence of a convergence between terrorist groups and organised crime groups.

Over the past 30 years, instances of systemic corruption linked to organised crime have been uncovered in Australian jurisdictions. However, Commissions of Inquiry have effectively publicised the corruption and proposed appropriate solutions, generally including the establishment of independent oversight bodies. Corruption undoubtedly persists in law enforcement and public sector agencies, but not of the nature or extent to challenge existing institutions. While domestic organised crime groups appear to have a general interest in corrupting selected public sector and law enforcement officers, they seem content to approach this in an opportunistic rather than systematic manner.

The main benefits to organised crime from public sector corruption are access to public funds and assets, rights and permissions, information, protection and platforms that facilitate other crimes. There is no evidence of large-scale direct infiltration of public sector agencies by organised crime groups. However, there is an ongoing threat of corruption of employees who work in areas that can facilitate illegal activities of organised crime groups, such as trusted insiders at Australian ports. This also includes people with access to information on the activities of other organised crime groups and law enforcement, and areas which can provide identification documents such as driver licences and other permits. Improper or inappropriate relationships with informants, as well as poor management of experienced criminals, remain corruption risks for law enforcement officers.

The potential for both political and public sector corruption increases, however, as organised crime identities extend their influence in the private sector, where they may influence decisions that will advance their corporate (and criminal) interests.

NON-TRADITIONAL ORGANISED CRIME MARKETS

The diversity of organised crime in Australia, and the methodologies used, challenges law enforcement and regulatory agencies to respond to threats from new areas, involving networks that bear little relationship to the popular concept of organised crime.

The front line against organised crime is increasingly in so-called 'grey markets' where legitimate and illicit economies meet and where the rules of engagement are determined by market forces, innovation, industry codes of conduct and regulation as much as by enforcement of the criminal law. Law enforcement agencies are developing broader and more diverse partnerships to respond to this threat. Some examples are included below.

HIGH TECH CRIME

Offences associated with technology-based crimes have rapidly developed due to the perception by offenders that there is a low risk of detection, and the high returns. Like most people engaged in organised crime, criminals using high tech means are motivated by financial gain. The difference is that they tend to operate as individuals or as loose-knit groups with little or no hierarchy. Online criminal enterprises have fluid memberships where members work together opportunistically. They prefer to work with certain individuals, based on trust, reliability and reputation. This can give the impression of a level of organisation and semi-permanence typical of traditional organised crime groups. However, many online offenders are offshore and their associations may be temporary,

remote and physically intangible. They operate in an environment of multiple international Internet service providers, complex international law and divergent legal requirements of countries whose citizens they target.

ENVIRONMENTAL CRIME

As with high tech crime, domestic criminal groups involved in environmental crimes are generally not organised in line with traditional models. Internationally there are increasing links between environmental crime and organised crime, but based on available intelligence this trend is not reflected in Australia. Criminal groups involved in environmental crimes in Australia demonstrate high levels of specialisation and have established networks, methodologies and illicit markets. Some have also been active for considerable periods. They meet a specific demand from a specific market and have no significant involvement in other criminal markets.

Officers from parks and wildlife services, environmental agencies and the Australian Quarantine and Inspection Service are as much stakeholders in this category of crime as law enforcement agencies.

The domestic risk posed by environmental crime remains stable, with no significant trends evident over the past year. However, awareness of environmental crime is increasing, with rising environmental consciousness, both here and overseas, and growing recognition of the need to protect the environment.

Environmental crime poses an increasingly diverse threat, both in terms of geographic spread and the range of crimes committed. For example, illegal dumping, wildlife crime and illegal fishing and logging are an increasingly global problem.

Organised crime has an international involvement in the illegal disposal of waste. Over the past 30 years, organised crime groups have dominated rubbish disposal for varying periods in parts of the US, the Italian city of Naples and parts of Germany and the Netherlands. During the same period some ostensibly legitimate companies with no links to organised crime competed with and replaced criminal companies but were also found to be acting illegally. Some customers seem prepared to tolerate the involvement of organised crime groups in rubbish disposal because they offer a lower-cost solution than legitimate companies which do not resort to illegal dumping.²⁰ There is nothing to suggest the same temptations could not apply in some niche areas of rubbish disposal in Australia, particularly rubbish that poses challenges in terms of safe disposal. At present there are only isolated examples of this occurring and no evidence that organised crime is centrally involved.



oil slick

²⁰ Ruggiero, V, 2010, *Organised Crime: Between the Formal and the Informal Economy*, Global Consortium on Security Transformation, Working Paper Series No. 4, July 2010.



Australia is predominantly an illegal exporter (rather than importer) of hazardous waste. This is a small-scale market and typically involves illegal exportation of electronic waste or lead-acid batteries.

Illegally logged timber and traditional medicines are two areas where Australia is considered an importer. These two components of environmental crime remain comparatively small compared with the illegal exportation of native flora and fauna.

Because of the unique nature of Australia's wildlife, illegal trafficking of native flora and fauna is mainly out of Australia. However, in some cases, Australian collectors are involved in the illegal importation of wildlife such as reptiles.

Challenges such as climate change invigorate organised crime because they force governments to divert resources from law and order to cope with natural disasters and scarcities of water or food. There are opportunities for organised crime groups to capitalise on shortages of critical resources and exploit complex financial processes designed to offset carbon production.

EXPLOITING CARBON TRADING SCHEMES

Organised crime groups in Europe have allegedly sought to exploit carbon trading schemes for criminal purposes.

In Norway, a group is being investigated for carbon tax evasion as part of a Europol tax fraud probe into allegations that up to five billion euros of revenue has been lost.

Cyber criminals also allegedly accessed European business systems and stole legitimate carbon trading permits, which were then sold on the open market. Trading was suspended for days until the problem was rectified.

Recent media reports suggest Italian organised crime groups are exploiting Europe's wind energy industry. Organised criminals are increasingly investing in the industry to qualify for subsidies and to launder proceeds of crime.²¹

Environmental damage is an inherent part of some organised criminal activity, including the production of amphetamine-type stimulants (dangerous chemicals are involved in production and toxic chemical residue is covertly dumped, including into waterways) and accessing the MDMA precursor chemical safrole (whole trees are destroyed to access their oil-bearing roots).

²¹ Pagnamenta, R, 2010, 'Organised Crime exploits wind industry', *The Times*, London, 9 August 2010, accessed 23 September <<http://www.theaustralian.com.au/business/industry-sectors/organised-crime-exploits-wind-industry/story-e6frg976-1225902848269>>.

CHILD SEX OFFENDING

As noted on page 27, advances in technology and the expansion of the Internet have enabled child sex offenders to become more sophisticated in their networking activities and more able to access information about offending techniques, possible victims and like-minded individuals.

CRIMINAL EXPLOITATION OF BUSINESS STRUCTURES

Criminals may use complex business structures to create confusion about the beneficial ownership of an entity. An effectively anonymous corporate entity offers substantial opportunities to conceal illicit funds and obscure the connection to the unlawful origin of those funds.

Organised criminal entities are increasingly using sophisticated networks of businesses, proprietary companies, partnerships and trusts to enable a range of organised criminal activities and regulatory offences—with repercussions for ordinary, unsuspecting citizens. Examples include revenue and taxation fraud, securities fraud, investment fraud, money laundering, ‘phoenix’ activity²², exploitation of the cash economy and non-compliance with industry legislation and statutory and award obligations.

There are general fears worldwide about criminals misusing corporate entities to disguise and convert the proceeds of crime, and concerns about the abuse of trust and company services to facilitate crime. This is recognised internationally by the inclusion of lawyers, accountants and trust and company service providers within the Financial Action Task Force (FATF) Forty Recommendations.²³ Australia is currently considering legislation to give effect to the relevant recommendation.

Although organised crime groups have not infiltrated the corporate and financial sectors in Australia to the extent of countries in Europe and the Americas, the level of infiltration is increasing and diversifying. Corporate entities are involved in a wide range of legitimate commercial activities and have a positive role in the growth of national economies, but under certain circumstances they can also be used for illicit purposes. Criminal exploitation of business structures typically involves the use of unlawful business practices and complex business structures to conceal criminal infiltration of an industry, to enable businesses to maintain or expand market share and to generate and conceal substantial licit and illicit profits.



22 Phoenix activity is defined as the evasion of tax through the deliberate, systematic and sometimes cyclical liquidation of related trading entities. This predominantly involves business operators seeking to preserve assets from creditors (including the Australian Taxation Office and employees) in order to continue in business.

23 The Financial Action Task Force (FATF) is a 34 member (including Australia) inter-governmental body which was established in 1990 to set standards and develop and promote policies to combat money laundering and terrorist financing. The FATF 40 Recommendations were drafted in 1990 and have been updated periodically since then. Recommendation 12 extends customer due diligence and record-keeping requirements to a number of non-financial institutions, including those listed above, in certain circumstances.

ORGANISED CRIME GROUP INVESTMENT IN THE LEGITIMATE ECONOMY

Vincenzo Ruggiero, Professor of Sociology and Co-Director of the Crime and Conflict Research Centre at Middlesex University in the United Kingdom (UK), argues that sophisticated organised crime groups may be forced to invest their proceeds in the licit economy because there are limits to the expansion of illicit markets, and because licit markets also provide an additional source for the growth of their power. Ruggiero notes that criminal entrepreneurs are encouraged by the conditions of semi-legality which exist in parts of most economies, and which in some cases are tolerated, so that the lines between licit and illicit activity become blurred, leading to what he calls 'dirty collar crime'.²⁴

Criminals are using corporate entities both to facilitate their criminal activity and sometimes as a criminal enterprise in itself. In some cases, organised crime is 'white-anting' legitimate businesses, with damaging effects on the original owners.

Widespread and systematic criminal exploitation of business structures may result in entrenched criminal activity within some industries. The harm associated with this is likely to be significant. Organised crime groups will increasingly exploit business structures to establish legitimacy and to distance themselves from their criminal activities, so that they can avoid attention from law enforcement and regulatory authorities.

Over the past several years a number of companies have been established primarily for the purpose of committing large-scale fraud. Some of these companies have been fronts for Ponzi schemes, while the principals and shareholders of others have engaged in securities fraud, money laundering and tax evasion.

Some professional advisers are contracted by organised crime groups, both knowingly and unknowingly, to facilitate organised crime. Other advisers form an integral part of organised crime networks. Professional intermediaries (solicitors, accountants, financial planners) facilitate money laundering through the financial system, obscure beneficial ownership and legitimise unlawfully derived funds. They can establish complex corporate and financial structures (both in Australia and overseas) to conceal and 'wash' criminally obtained funds.

Australian companies and individuals have used professionals and offshore businesses to facilitate the transfer of income to overseas secrecy havens, using sometimes complex business structures.

²⁴ Ruggiero, *Organised crime: between the formal and the informal economy*, pp12-14.

AUSTRALIAN SOLICITOR JAILED FOR FACILITATING TAX EVASION

Australian solicitor Paul Gregory was found guilty in February 2010 of conspiring with promoter and entertainment manager Glenn Wheatley and principals of the Swiss-based accounting firm Strachans SA to cause a risk of loss to the Commonwealth. In March 2003 Gregory was found to have sent an email to Strachans SA which, the court held, was a calculated deception to enable Wheatley to evade his tax. Upon conviction, Gregory received a custodial sentence, one of a number arising from the multi-agency taskforce, Project Wickenby.²⁵

There is evidence of links between phoenix activity and organised crime. Phoenix activity occurs when directors of a company that is about to be liquidated transfer assets to another company which they also control. This leaves no assets to pay creditors but enables the business to continue under the new company. Complaints concerning phoenix activity are increasing in Australia and the activity is being used to avoid tax and superannuation liabilities in a range of industries. Professional facilitators such as insolvency practitioners, solicitors and tax agents have been identified as assisting individuals to take part in phoenix activity.

Phoenix activity has historically been most prevalent in small, labour-intensive, cash-focused businesses with a turnover below A\$2 million and this remains the case. Recently, however, phoenix activity appears to have spread into the higher end of the small and medium enterprises market segment. It is also beginning to emerge in sectors such as property development and finance. Particularly vulnerable industries

include the private security, building and construction, entertainment, telecommunications, property development, labour hire, employment, road transport

and cleaning industries. The Australian community bears a significant part of the cost of phoenix activity through reduced tax revenue. It is used to avoid a range of taxes including income tax, goods and services tax and superannuation guarantee obligations. State tax authorities may also be adversely affected by phoenix activity.

“Criminals are using corporate entities both to facilitate their criminal activity and sometimes as a criminal enterprise in itself. In some cases, organised crime is ‘white-anting’ legitimate businesses, with damaging effects on the original owners”

²⁵ R v Gregory [2010] VSC 121.



Some investment fraud involves substantial planning and organisation and uses sophisticated methods and techniques. Professional facilitators such as lawyers, accountants and money remitters play a key role in providing access and opportunity for criminals. As regulations are tightened, this specialised involvement is likely to increase.

Agencies that are stakeholders in relation to this type of offending include the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, the Australian Taxation Office, the Australian Federal Police, Treasury and Finance departments and other agencies responsible for regulating the finance sector and industries affected by the activity. The effective operation of the business and financial sectors is integral to a prosperous economy and the intrusion of organised crime groups is cancerous and difficult to remove once it has taken root.

ENABLER ACTIVITIES

Enabler activities—often criminal activities in their own right—facilitate other types of organised crime. The threat and harm they pose therefore multiplies, from the criminality of the core activity to the ripple effects in other crime markets.

Enabler activities examined are:

- > identity crime
- > money laundering
- > violence
- > high tech crime.

IDENTITY CRIME

INTRODUCTION

Credit card fraud, Internet scams to elicit banking and personal details, identity theft, social security fraud—identity crime is one of the ways in which serious and organised crime reaches into many ordinary businesses and homes.

Identity crime is a common element in serious and organised crime and poses a critical risk to the Australian community. Fraudulent identification is used to cheat unsuspecting victims, conceal criminal activities and movements and evade detection or arrest.

Advances in information and communications technology provide unprecedented opportunities to exploit greater numbers of people with each new criminal scheme.

DISCUSSION

Identity crime encompasses the theft of identity information and related financial information, the assumption of another identity for fraudulent purposes and the production of false identities and financial documents to commit crimes. The main targets for fraudulent identity documentation are banks, lending agencies and other financial institutions and taxation/revenue collection agencies. Organised crime groups which engage in identity crime take advantage of weaknesses in identification and authentication processes. Identity crime allows them to avoid taxation, obtain fraudulent loans and withdraw funds illegally, open and operate bank accounts in false names for the purpose of money laundering and facilitate organised theft by shopping groups using false credit cards and skimmed card data.





Identity crime is also evident in taxation fraud, where false identities are used to lodge fraudulent tax returns for refunds. By using someone else's identity, the perpetrator attempts to remain anonymous and at arms length from the fraud.

Identity crime is both a crime type in its own right (at least at state level)²⁶ and an enabler of other crime types. Syndicates have become professional identity crime 'specialists', with the single purpose of producing high-quality fraudulent identity documents. Identity crime enables other crime types in two ways:

- > false or fraudulent identities make it more difficult to identify who is committing offences
- > identity crime provides a means of financing activities such as money laundering, people smuggling, terrorism, fraud and drug trafficking.

Intelligence indicates that specialist groups operate large-scale identity production facilities in Australia, providing documents to criminal syndicates. Identity crime groups use both sophisticated, cost-effective technology and simple 'off-the-shelf' products to produce identification and credit cards that replicate overt and covert security features.

Mail theft remains one of the enablers of identity crime. Personal information continues to be regularly sent through postal services and, even though there are security processes protecting this information, some criminal groups are likely to continue using the post to obtain identifying documents and particulars.

Card skimming—the theft and use of identification data from financial transaction cards—is now considered a prominent feature of the identity crime market. Card skimming is becoming more structured, with overseas and domestic groups involved. It allows criminal groups to launder funds and to buy goods and sell them for profit. It also supports other offences such as card fraud²⁷ and is a source of funding for other crime types.

Identity crime is likely to increase in the future. A number of factors are expected to influence this, including technological advances increasing high-speed information flows (which will allow criminal groups to share information faster and may make detection more difficult), increased use of wireless remote communications, and the lack of widespread biometric identification measures (such as those which incorporate fingerprints).

²⁶ Identity crime is not technically a crime at Commonwealth level at present, although provisions currently before the Commonwealth Parliament will make identity theft a crime.

²⁷ Due to the prevalence of skimmed card identity data in card fraud, this subject is more fully assessed in the 'Crimes in the mainstream economy—Card fraud' section of this report.

As an enabler, identity crime can obscure the nature and identity of people who commit other crimes—ensuring it will remain a feature of the organised crime environment. The growth of identity crime will also be driven by the nature, diversity and evolution of identity crime syndicates and offences.

However, there may be some inhibitors to slow the momentum. If chip and PIN technology is more widely operational in Australia as expected by 2013, it should reduce card skimming. If biometric measures are introduced on a broader scale and government-endorsed document verification schemes continue to be implemented, this should also slow the growth of identity crime.

Government initiatives may also slow the growth of identity crime. For example, the Government is working with the states and territories to implement the National Identity Security Strategy (the Strategy) agreed to by the Council of Australian Governments to strengthen identity management processes to prevent and combat crime. The Strategy includes measures to improve standards and procedures for verifying consumers' proof of identity when registering for government services, enabling the general public to have greater confidence in using government services online, and enhancing interoperability of biometrics.

The Government has introduced new legislation (the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2010) which inserts identity crime offences into the Commonwealth Criminal Code and includes measures to assist victims of identity crime.

As the banking and finance sectors are increasingly being targeted by cyber and identity crime, the Government is engaging with those sectors to develop a collaborative partnership to prevent identity crime, in particular the harm caused by credit card fraud. A multi-agency Identity Crime Implementation Team has been established to develop policy and operational responses to identity crime.

The Government also undertakes public campaigns to raise awareness of identity crime and how to protect a person's identity. Examples of this include the 2010 National Fraud Awareness Week, which included more than 100 partners from government, the private sector and the community, and the release of a booklet titled *ID Theft – Protecting your Identity*.





MONEY LAUNDERING

INTRODUCTION

Organised crime groups rely on money laundering as a key way of legitimising or hiding proceeds or instruments of crime.

Money laundering is a pervasive, corrupting process that can blend criminal and legitimate activities. It stretches across areas as diverse as mainstream banking, international funds transfers and foreign exchange services, gambling, shares and stocks, artwork, jewellery and real estate.

DISCUSSION

Financial profit is the main driver for organised crime groups and greed and power are their key motivation. Legitimising the proceeds of crime and the instruments of crime (the means by which crime is committed) is therefore crucial for organised crime and this activity poses an ongoing risk.

Through money laundering, criminals attempt to hide and disguise the true origin and ownership of the instruments of crime and the proceeds of crime so they can avoid prosecution, conviction and confiscation of criminal funds. Money laundering offences are defined in Part 10.2 of the *Criminal Code Act 1995 (Cwlth)*. The offences encompass a very wide range of criminal activity.

Money laundering is an extremely diverse activity. It is carried out in Australia at all levels of sophistication by most, if not all, organised crime groups, with or without the assistance of professional advisers, and using a constantly evolving variety of techniques. No single industry sector, financial product or profession is consistently exploited by organised crime groups.

Contemporary estimates suggest that the level of money laundering in and through Australia is at least A\$10 billion a year. Although it is thought the actual figure may be higher, the absence of an agreed methodology for estimating money laundering and gaps in information on the financial dimension of organised criminal activity hamper efforts to calculate an accurate figure.

Common methodologies used to move proceeds and instruments of crime across borders are:

- > mainstream banking channels
- > the cross-border movement of bullion, jewellery and bearer negotiable instruments
- > cash smuggling
- > international remittance and foreign exchange services (corporate and alternative remittance dealers)
- > money laundering schemes involving secrecy havens.

In Australia, syndicates have been identified laundering funds by storing large amounts of cash in secure locations, gambling at casinos and other venues or online, intermingling criminal and legitimate activities, investing in a range of high-value assets such as cars, motorcycles, marine craft, racehorses, works of art, jewellery and real estate, investing in securities, shares and stocks, operating bank accounts in false names and transferring assets to non-criminal associates.

Three key factors influence the selection of particular money laundering methodologies: efficiency, capacity and cost. On this basis, organised crime groups continue to widely use alternative remittance dealers. International funds transfers by some dealers can conceal their clients' illicit money flows among the high volumes of aggregated (mainly legitimate) daily transactions.

RESPONDING TO THE THREAT POSED BY ALTERNATIVE REMITTANCE SERVICES

Australia has recently adopted stronger enforcement measures in recognition of the threat posed by some alternative remittance services. Under section 229 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the Chief Executive Officer of the Australian Transaction Reports and Analysis Centre (AUSTRAC) may make written Anti-Money Laundering and Counter-Terrorism Financing Rules. The Rules are binding legislative instruments. The recently registered Rule 44 permits the AUSTRAC Chief Executive Officer to de-register high-risk money remitters.

On 11 November 2010, the Government released for public consultation the Exposure Draft of the Combating the Financing of People Smuggling and Other Measures Bill. The draft Bill amends the AML/CTF Act to introduce a more comprehensive anti-money laundering and counter terrorism financing regulatory regime for the alternative remittance sector. In particular, the measures in the draft Bill:

- > introduce AML/CTF regulation of providers of remittance networks: organisations that establish the network systems used by agents to facilitate customers' funds transfers internationally
- > provide the AUSTRAC CEO with the ability to refuse, suspend, cancel or impose conditions on the registration of remittance network providers and remittance dealers
- > provide AUSTRAC with greater enforcement powers by extending the infringement notice scheme to cover certain breaches of registration requirements by the alternative remittance sector.

The Government introduced the draft Bill into Parliament during the Autumn 2011 sittings period.

Identity crime increases the level of risk posed by money laundering as it enables offenders to operate accounts, hold assets, transfer funds offshore and generally avoid detection when dealing with proceeds of crime. The range of laundering options for criminal groups is wide and increasing. Significant drivers include the input of professional advisers located both within the jurisdiction and offshore.

Trade-based money laundering and bulk cash smuggling are international concerns that have been identified as emerging or possible threats in Australia. International trade provides criminal syndicates with the opportunity to launder money.²⁸ The international trading system is attractive for money laundering due to the enormous volume of trade flows, the complexity associated with foreign exchange transactions, and the additional complexity associated with commingling illicit funds with the cash flows of legitimate businesses.

Throughout Europe and North America, organised crime groups continue to use cash smuggling as a primary method of moving illicit funds. The anonymity and relative simplicity compare favourably with the specialist knowledge or complicity required for alternative methods in the finance sector. Although not seen in Australia to date, internal physical concealment of cash has been identified internationally, with amounts up to 350,000 euros being detected.

Further assessment is required to determine the extent of organised criminal exploitation of other sectors or methods that offer opportunities for money laundering including self-managed superannuation funds, hedge funds located in overseas secrecy havens, pre-paid or stored value cards, online payment systems, online gambling and online 'virtual worlds' and gaming platforms.

“Financial profit is the main driver for organised crime groups and greed and power are their key motivation. Legitimising the proceeds of crime and the instruments of crime (the means by which crime is committed) is therefore crucial for organised crime and this activity poses an ongoing risk”

²⁸ Trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.

THE AUSTRALIAN LEGISLATIVE AND REGULATORY FRAMEWORK

The Australian regulatory framework in relation to money laundering has multiple hierarchical legislative layers. The first layer is specific anti-money laundering legislation, with secondary layers of taxation, banking, superannuation and corporation laws. The Australian anti-money laundering regulatory regime has been developed in conjunction with international regulatory schemes implemented under international instruments for combating transnational crime and organised criminal groups. To strengthen existing arrangements, amendments were recently made to the *Proceeds of Crime Act 2002 (Cwlth)* to target criminal business structures, including the financial and material assets of criminal entities—recognising that such measures are crucial to disrupting organised crime. The amendments introduce a range of measures (principally ‘unexplained wealth’ provisions) to extend and enhance the Commonwealth asset confiscation regime. These measures are intended to increase the capacity of the Commonwealth to successfully respond to organised crime by targeting wealth derived from criminal activity.

It is estimated that the regulated industry sectors exposed to money laundering consist of:

- > 1 400 authorised deposit-taking institutions and other lenders
- > 3 800 non-banking financial service providers such as planners, fund managers, stockbrokers and custody, superannuation and life insurance providers
- > 5 500 gambling and bullion entities such as casinos, TABs, hotels, clubs, online gambling providers, bookmakers and bullion dealers
- > more than 6 500 money service businesses, including alternative remitters, cash carriers and foreign exchange dealers.

Organised crime will consistently seek to exploit areas that receive less regulatory attention. Collectively, domestic groups and individuals who launder the proceeds of crime demonstrate a significant capability to change and adapt in response to increasing regulatory controls. While they vary in sophistication, they are able to purchase specialist advice, exploit corporate structures and conceal this activity within myriad legitimate financial transactions.

The strong regulatory controls for mainstream financial institutions may displace criminal attention towards products and services considered to attract less regulatory focus. Accordingly, less regulated parts of the Australian financial sector, and offshore jurisdictions with high levels of organised crime and limited national anti-money laundering controls, are areas of ongoing vulnerability for Australia.



The fight against money laundering is led by AUSTRAC, with key roles played by Commonwealth, state and territory law enforcement and public sector agencies responsible for regulating and monitoring the financial sector. The private sector also has an important (and broadening) role due to the variety of methods organised crime groups are using to launder the proceeds of crime. AUSTRAC's significant role in this regard is to ensure compliance with Commonwealth legislation. The response to money laundering underlines the benefits of broader partnerships between law enforcement and the public and private sectors.

The critical risk posed by money laundering is likely to continue because it is an inherent organised criminal activity.

VIOLENCE

INTRODUCTION

Rivalry between organised crime groups at times spills over into highly visible violence, sometimes with innocent bystanders as victims.

However, the use of violence among organised crime groups is more widespread and insidious than such high profile incidents. Violence or the threat of violence is used 'strategically' to punish, intimidate or coerce people into committing or assisting criminal activities, to pressure witnesses or to recover debts.

DISCUSSION

The use or threat of violence remains an enabler and integral part of organised criminal activity. The level of control and effectiveness of the use of violence depends on the type of group and its relationships with other crime groups. Some seek to use violence in considered, measured ways to achieve a particular outcome or profit, while those with 'brotherhood' characteristics may also use violence to settle matters and maintain honour and status. Still others encourage a range of violence, often centred on 'contract violation', to recover debts or to retaliate for failure to supply agreed goods. Consequently, violence between competing organised crime groups centres on matters of honour and reciprocal action, competition over territory or markets, enforcing illicit contracts and internal discipline. Congruent with this is the emergence of groups who specialise in this crime type and are 'for hire'. This provides an easy source of income and can draw less attention compared with other crime types such as drug trafficking.

Although violence may be used strategically, it is also frequently opportunistic or without significant thought of gaining profit or advantage, sometimes without regard for consequences. There is ongoing evidence of violence motivated by personal revenge and retribution, particularly by Middle Eastern organised crime groups, which often leads to further violence. Thus, violence by organised crime groups is less predictable and more opportunistic today than it has been historically.

Increased violence by organised crime groups in some jurisdictions during 2009—including the violent incident at Sydney Airport and subsequent related attacks—appears to have reverted to more historical (lower) levels. This is probably a result of law enforcement investigations into groups that were prominent in a number of the violent incidents and an effort by some organised crime groups to limit the public attention being drawn to their activities.

Rival crime groups and people associated with the activities of organised crime groups are the main targets of violence and threats to use violence. However, there is also a constant risk that members of the public will become the unintended victims.

Violence, extortion and threats of violence are used to intimidate people and pervert the course of justice by preventing witnesses from assisting police or giving evidence in court. Kidnapping and threats of violence are also tactics used to discourage people from assisting law enforcement or rival groups. Organised crime groups usually target other criminals because they are considered less likely to report violence to law enforcement. People who have fallen out with senior organised crime identities, or whose usefulness has ended, have also been kidnapped, threatened or even murdered. The extent of this type of offending is unclear, but is likely to be significantly higher than reported.

Certain groups are more prepared to use violence and go to greater lengths than others. For example, the deliberate use of violence is a key feature of Middle Eastern organised crime groups. A case in point: persons, particularly of Lebanese background, have significantly escalated the level of violence within and between outlaw motorcycle gangs since they have become members over the past decade. There is evidence that outlaw motorcycle gangs members, regardless of ethnicity, are prepared to use violence to protect the membership and areas of influence of their particular chapter and group. ‘Patching over’²⁹ of members from one outlaw motorcycle gang to another has caused significant problems in several jurisdictions. In most cases, local police provide the primary response to incidents of violence, but the causes of and motivation for such incidents may have broader implications, particularly where the violence is being employed as a considered tactic.

²⁹ The process whereby a member of one outlaw motorcycle gang is invited to renounce that membership and become a member of another outlaw motorcycle gang.



HIGH TECH CRIME

INTRODUCTION

Use of computers and the Internet is now intertwined with many aspects of daily life, from online transactions and social networking to using email and browsing the web. This is creating new vulnerabilities that organised crime groups are quick to exploit. Criminals are using new and converging technologies to facilitate crimes such as identity theft, money laundering, sale of illicit or counterfeit goods, mass marketing fraud and credit card fraud.

DISCUSSION

Statistics about the size of the Internet and level of Internet and email use provide an appropriate context for assessing the potential for high tech crime to occur and increase. Eric Schmidt, the Chief Executive Officer of Google, estimates that the Internet has five million terabytes, or five billion gigabytes, of data and that the quantum of data is increasing at the rate of 100 terabytes per month.³⁰ By way of comparison, the human brain holds some 10 terabytes of data.

At the end of 2009 there were an estimated 1.73 billion Internet users world-wide. This included 47 million who were added during 2009, of which 21 million were located in Oceania/Australia. During 2009, 90 trillion emails were reportedly sent world-wide (an average of 247 billion a day) by a total of 1.4 billion email users. Eighty-one per cent of all emails sent were 'spam' (unsolicited bulk email), an average of 200 billion each day. An additional 148 000 new 'zombie' computers were allegedly created each day as part of botnets to send spam around the world. There were at least 2.6 billion malicious code threats (including viruses and 'trojans') at the start of 2009 and more than 921 000 new malicious code signatures were added by Symantec during the final quarter of 2009.³¹

High tech crime takes two forms: crimes that use technology to facilitate the commission of an offence (for example, using a carriage service to access child pornography) and offences that could not have occurred without technology (such as unlawful access and system impairment). Traditional organised crime groups use technology to communicate and to facilitate crimes such as drug trafficking, money laundering, extortion and fraud. There is limited evidence that Australian-based organised crime groups are directly attacking computers and computer systems.

³⁰ <<http://www.wisegeek.com/how-big-is-the-internet.htm>>, viewed 30 November 2010.

³¹ <<http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/>>, viewed 30 November 2010.

High tech crime includes attacks on computers and computer systems. It has spawned industrial espionage and enabled denial of service attacks and the impairment of critical systems that can impact on national security and economic stability.

The principal threat to Australia from high tech crimes remains offshore. The threat is from temporary and opportunistic networks, consisting of people who operate as individuals or as loose-knit groups with little or no hierarchy. These online criminal enterprises are often well resourced and have fluid memberships.

As noted by the Commonwealth Attorney-General, Robert McClelland, in September 2010,³² computers and the Internet are now linked with almost every facet of our lives and this electronic connectivity has created new vulnerabilities. A serious attack on networks that control key systems in our economy (banking and finance systems, water or electricity grids or mobile phone networks) could have devastating consequences, as would major disruptions to the flow of information across the Internet itself.

Attacks against computers are becoming more sophisticated and common. Criminals without strong technological skills are obtaining ready-made malicious software packages online to commit a range of offences. Criminal methodologies are also available on underground websites and in 'chat rooms'. Criminal groups are moving away from traditional methods of infecting victims' computers through spam emails; instead they are using emails to divert victims to facsimiles of familiar commercial websites that in fact contain embedded malware.

Aspects of the card skimming process converge with high tech crime. Card skimming is becoming more sophisticated, with groups sending identity data skimmed in one country to groups in another country to use. Skimmed identity data flows both in and out of Australia. The gradual move towards chip and PIN technology over the next two years should reduce domestic card skimming, but it may displace criminal activity to other more vulnerable areas of the market, such as card-not-present fraud (see more information on pages 26 and 27).

Cyber security threats to critical systems are currently investigated and monitored by national security agencies (primarily through the Cyber Security Operations Centre), law enforcement agencies (particularly the Australian Federal Police) and public and private sector agencies. Much of the key infrastructure, systems and hardware is privately owned and operated. Both the public and private sectors invest heavily in measures to minimise the impact of high tech crime and to protect key national infrastructure from external attack. The risk posed by high tech crime is likely to increase in the short- to medium-term.



³² Speech delivered at the launch of Cyber Storm III in Canberra on 29 September 2010.

CRIME MARKETS



crack cocaine

Analysis of crime markets provides valuable insights into organised crime activity, trends and vulnerabilities. Greater understanding supports more effective use of resources against serious and organised crime.

Crime markets examined are:

- > illicit drug markets—for example, cocaine, methylamphetamine and MDMA
- > other illicit commodities—for example, firearms and counterfeit goods
- > crimes in the mainstream economy—for example, superannuation fraud, insurance fraud and health fraud
- > crimes against the person—for example, people trafficking.

ILLICIT DRUG MARKETS

Illicit drug use leads to serious economic and social harm across the whole community. It affects not only those using the drugs, but often also damages families and friends.

Illicit drug markets are the most profitable of the organised crime markets in Australia and the principal source of profit for organised crime groups. Australia is an attractive environment for suppliers and producers of illicit drugs for several reasons. Australians are among the world's highest per capita consumers of illicit stimulants, and drug prices in Australia far exceed prices overseas, making domestic drug production and importation highly profitable.

Using illicit drugs in the company of friends and associates on social occasions, and drug dealing within social networks, have become accepted behaviour in some circles—particularly involving illicit stimulants such as methylamphetamine, MDMA, cocaine and analogue substances that mimic the illicit stimulants. A 'pill culture' has evolved along with this shift.

The major illicit drug markets in Australia are multi-billion-dollar enterprises that provide an opportunity for significant numbers of syndicates to operate.

COCAINE

THE INTERNATIONAL SITUATION

Cocaine is produced from the leaves of the coca plant, which is native to South America. Cocaine production is centred in Colombia, Peru and Bolivia, so the drug has to be imported into Australia. Sizeable cocaine markets are now established throughout Europe and North and South America, with cocaine being transhipped through Africa, the Pacific, Central and North America and North and South-East Asia. Accordingly, cocaine arrives in Australia from many intermediate locations, although the majority of cocaine detected at the Australian border continues to be imported directly from North and South America.

The drug's global presence has broadened opportunities to acquire and traffic cocaine. This is reflected in the broad range of criminal groups now involved in large-scale and opportunistic cocaine trafficking ventures, both domestically and internationally.

The global cocaine market remains robust. Although cocaine use in the US has been in decline for up to a decade, the situation in Europe is less clear. Cocaine use appears to have stabilised in some Western European countries and the UK. A recent inquiry into the UK cocaine market suggested a two-tier market may have developed, with less pure but cheaper cocaine being marketed to users who were previously unable to afford it.³³

Supply reduction strategies in South America, including crop eradication, will always be the key to reducing world cocaine supplies. There are signs that supply reduction strategies in Colombia are meeting with some success. However, reports from Bolivia suggest that Colombian and Mexican criminal groups are investing capital in Bolivia and Peru to support coca production in these countries and ensure there are sufficient supplies of cocaine to satisfy market demand. Networks involved in the production and international trafficking of cocaine are among the most sophisticated, profitable and powerful criminal networks in the world. They have displayed considerable ingenuity and invested heavily in concealment methods designed to avoid detection of cocaine importations.

³³ UK House of Commons Home Affairs Committee 2010, *Seventh Report: the cocaine trade*, 23 February 2010.



coca plant



CONCEALMENT METHODS USED BY SOME SOUTH AMERICAN CRIMINAL SYNDICATES

South American-based criminal syndicates responsible for global cocaine distribution are committing extensive resources to develop technologies to circumvent detection. Although authorities report numerous concealment methods for powdered product, European authorities have identified an increasing number of sophisticated processes which incorporate cocaine into a range of processed goods (such as fertiliser, clothing, beeswax and food oils), from which it may later be recovered in illicit 'secondary extraction' laboratories. A notable example was revealed in the Netherlands where a consignment of eight tons of shredded plastic was detected at such an extraction site. Examination revealed that cocaine had been chemically embedded in the plastic. Subsequent investigations revealed that more than 50 tonnes of this plastic product had been imported previously from Colombia.

A variety of primary and secondary data indicates cocaine consumption is increasing in Australian society. Given the considerable volume and variety of traded materials imported into Australia annually, the technique of distributing cocaine through impregnated substances will present a significant challenge to Customs and Border Protection detection strategies. Attempts have been made to import cocaine into Australia using impregnated plastic, although not on the scale of the Dutch example.

In terms of transnational supply routes, West Africa remains a problem. Despite international efforts to combat drug trafficking through the region, an estimated US\$1 billion worth of cocaine continues to be trafficked through West Africa. A number of international criminal groups have established a presence in West African countries to facilitate worldwide cocaine distribution.

THE DOMESTIC SITUATION

According to Australian national drug user surveys, cocaine use is at historically high levels. Cocaine arrests are also at historically high levels. Law enforcement agencies have identified increasing availability throughout Australia, despite the fact that the price of cocaine in Australia is significantly higher than in many overseas markets.

Because of the variety of international transshipment routes, an increasing range of criminal groups are able to access cocaine for importation into Australia.

However, criminal groups from, or with links to, Central and South America—and those groups already established in the Australian cocaine market—are expected to maintain a competitive advantage in trafficking the drug into Australia. Mexican criminals have become more prevalent as principals in the importation and supply of cocaine and associated money laundering. There is concern that they may also import the violent practices which have been reported overseas.

There is increasing evidence that the harm from cocaine use is significant. A recent inquiry into the cocaine market in the UK stated: ‘Medical understanding of the precise nature of harm associated with regular cocaine powder use is still developing; but a body of evidence is emerging about the links to heart disease, the long-term erosion of cognitive brain function, and of disturbing toxic effects when combined with alcohol, when it forms a third substance, coca ethylene, more dangerous than either of the two ingredients.’³⁴

In Australia, the social costs (health effects, crime costs and road accident costs) of cocaine were estimated to be approximately A\$300 million a year. This was significantly lower than for other illicit drug markets in Australia (for example, the social costs of opiate use were estimated at A\$4.5 billion dollars and the cannabis market at A\$3.1 billion).³⁵

It is difficult to accurately assess and measure the cocaine market in Australia because of the relative lack of data compared with other illicit drug markets. One factor is that a significant proportion of cocaine users are not captured through research techniques that have traditionally been used to monitor Australian illicit drug markets. Innovative and tailored research and intelligence collection is needed to permit a more comprehensive understanding of the Australian cocaine market. It is likely that the risk posed by the cocaine market will increase in the short- to medium-term.

METHYLAMPHETAMINE

Most methylamphetamine³⁶ consumed in Australia is produced locally. However, some forms of methylamphetamine and most precursor chemicals used to produce methylamphetamine are imported, so it is necessary to consider both international and domestic factors.

The methylamphetamine market remains highly functional, resilient and entrenched, with domestic criminal individuals and groups having established extensive domestic and international criminal networks.



“Ice” (crystal methamphetamine hydrochloride)

34 House of Commons Home Affairs Committee, 2010, *The Cocaine Trade: Seventh Report of Session 2009–10*, London.

35 Social Research Centre 2008, *Research report: National Drugs Campaign: evaluation of Phase Three, April 2008*, Social Research Centre, Melbourne, p. 31 <[http://www.drugs.health.gov.au/internet/drugs/publishing.nsf/Content/123BCCoBA8FF2366CA25759B00059D63/\\$File/nidc_eval3.pdf](http://www.drugs.health.gov.au/internet/drugs/publishing.nsf/Content/123BCCoBA8FF2366CA25759B00059D63/$File/nidc_eval3.pdf)> viewed 19 February 2010.

36 Forms of methylamphetamine are referred to colloquially by a number of names: the powder form is generally known as ‘speed’, the paste form as ‘base’ and the crystal form as ‘ice’.



clandestine laboratory

A range of criminal groups produce and distribute methylamphetamine in Australia as well as importing some forms of methylamphetamine and precursor chemicals. Among them are Australian-based members of outlaw motorcycle gangs, Middle Eastern, Eastern European and West African criminal groups, and individuals and criminal groups of South-East Asian extraction. Domestic criminal groups and criminal groups based in South-East Asia maintain a competitive advantage in the trafficking of crystal methylamphetamine (ice) into Australia.

Methylamphetamine use is no longer increasing, with primary national drug user surveys showing sustained decreases in reported use in recent years. Methylamphetamine remains readily available, but some jurisdictions have identified volatility in the market, with low purity and high prices.

Domestic production of methylamphetamine remains robust,³⁷ with criminal individuals and groups innovating and adapting in response to the increasingly strict regulation of precursor chemicals. Examples include:

- > targeting medication containing pseudoephedrine in pharmacy break-ins
- > using false identities to obtain medication containing pseudoephedrine at a series of pharmacies ('pseudo-running')
- > 'doctor shopping' to secure pseudoephedrine medications in bulk by prescription
- > disguising key drug precursor chemicals by transforming them into new non-controlled substances for international shipment, then reversing the masking process to liberate the controlled chemical
- > developing new manufacturing processes which are based on non-regulated substances.

Methylamphetamine is consistently identified as being pressed into tablets and marketed as MDMA (ecstasy). The low to sporadic availability of MDMA, if sustained, is likely to see strong demand for methylamphetamine among organised crime groups involved in pressing it into tablets.

PRECURSOR CHEMICALS

Precursor chemicals are an essential part of the production process for methylamphetamine. The chemicals differ according to which production process is used. Large amounts of precursor chemicals continue to be detected at the border, and to be diverted domestically from a range of sources. The People's Republic of China, Thailand, Cambodia and India are primary sources

³⁷ Between 2007–08 and 2008–09, the number of amphetamine-type stimulants clandestine laboratory detections increased 14 per cent and between 2008–09 and 2009–10 the number of detections increased a further 54 per cent, from 449 to 694. However, caution should be exercised in interpreting this data as this may reflect enhanced law enforcement capacity and improved detection methods. The capacity of clandestine laboratories also needs to be considered in any interpretation of the data.

for the Australian illicit precursor market, although enforcement action in China³⁸ is resulting in criminal groups increasingly sourcing precursor chemicals from India. Myanmar, Bangladesh and Malaysia have also been identified as emerging sources of illicit precursor chemicals. In the short- to medium-term, international and domestic criminal groups are expected to maintain a prominent role in trafficking and diversion of precursor chemicals.

METHYLAMPHETAMINE-RELATED HARMS

In the most recent National Drug Strategy Household Survey, 16 per cent of persons aged 14 or older considered methylamphetamine or amphetamine use to be of most serious concern for the general community. This was the highest rating of the listed illicit drugs, followed by heroin (which was combined with cocaine as a category). To put this in context, excessive drinking of alcohol was considered of most serious concern for the general community (at about 32 per cent) and the next highest concern was tobacco smoking (at 17 per cent).

From 1993–2007, amphetamine-related hospital separations³⁹ were second highest among the illicit drug types examined in the study. Nationally, these separations have steadily increased throughout the 14-year period of data collection. In 2007–08, amphetamines⁴⁰ were the third most common principal drug of concern for which treatment was sought, accounting for 11 per cent of episodes. In 2007, the estimated social cost (health effects, crime costs and road accident costs) of methylamphetamine use was A\$3.7 billion per annum. The social cost of methylamphetamine use was the second highest of the illicit drug markets (see footnote 35).

MDMA (ECSTASY)

Most MDMA⁴¹ consumed in Australia is imported. Although Western Europe remains a source of MDMA, production is now occurring throughout Eastern Europe, South-East Asia and Canada. MDMA is also produced in Australia. The relative market share of domestic versus imported MDMA consumed in Australia remains difficult to determine. However, the limited scale of production detected in Australia to date suggests that imported MDMA remains the primary source for the Australian market.



MDMA (ecstasy)

38 According to China's National Narcotics Commission there are about 130 000 producers of precursor chemicals in China. Between 2005 and 2008, 5053 tonnes of chemicals were prevented from being illegally exported. <www.news.xinhuanet.com/english/2009-10/12/content_12219281.htm>, viewed 23 November 2009.

39 A hospital separation is defined as an episode of care for an admitted patient, which may refer to a total hospital stay, or a portion of a hospital stay beginning or ending in a change of type of care, or transfer to another hospital. The term 'amphetamine' is used in the original data set and is therefore used for accuracy; however, the terms 'amphetamine' and 'methylamphetamine' are interchangeable.

40 Defined for this study as amphetamine, methylamphetamine, dexamphetamine and amphetamines not elsewhere classified.

41 As opposed to the increasingly common situation of other substances being sold as MDMA.

Domestically, and in many countries around the world, the purity of tablets marketed as MDMA has been decreasing, with a range of other substances being pressed into tablets and sold as MDMA. A global shortage of 3,4 MDP2P, a precursor chemical required for the synthesis of MDMA, is believed to be one of the main reasons for the decrease in quality of MDMA tablets. Large seizures

of MDMA continue to be reported overseas, suggesting that MDMA remains available, yet supply is insufficient to satisfy global demand.

There are indications that MDMA is becoming increasingly available following ongoing instability in the market in Australia throughout 2010. However, the market is re-developing slowly and high-quality MDMA remains largely unavailable.

“The direction of the MDMA market will be a primary driver of future trends in other illicit markets in Australia”

Latent demand for high-quality MDMA remains strong, but the large number of low-purity or inactive tablets sold as MDMA appears to be resulting in some users moving away from using such tablets. However, the domestic MDMA market is expected to quickly re-establish if the purity of MDMA tablets increases or high-quality MDMA becomes readily available in Australia.

The future trajectory of the MDMA market in Australia remains difficult to assess and will be influenced significantly by international trends and the availability of high-quality MDMA. The direction of the MDMA market will be a primary driver of future trends in other illicit markets in Australia and may result in users switching to a range of other drugs.

The main criminal groups identified as trafficking MDMA into Australia and distributing it around the country are Eastern European criminal groups, Italian and Western European criminal groups, Israeli criminal groups, South-East Asian criminal groups and Australian-based criminal groups including outlaw motorcycle gang members.

South-East Asian criminal groups dominate the production of MDMA in Canada and throughout South-East Asia. In July 2009, a joint UN Office on Drugs and Crime–Interpol team identified facilities in West Africa which contained stockpiles of MDMA precursor chemicals and an industrial scale high pressure vessel. The UN Office on Drugs and Crime has raised concerns over the potential for West Africa to emerge as a source country for MDMA.⁴² With West African criminal groups active in Australia, the potential exists for these groups to diversify into trafficking MDMA into Australia.

⁴² United Nations Office on Drugs and Crime, 2009, *Global smart update 2009, volume 2*, United Nations, Vienna, p.6.

MDMA PRECURSOR CHEMICALS

Because of the global shortage of 3,4 MDP2P, criminal groups have increasingly targeted safrole (the natural product from which 3,4 MDP2P is manufactured) as the starting material for the synthesis of MDMA. In February 2009, 15 tonnes of safrole was destroyed in Cambodia by law enforcement agencies including the Australian Federal Police, to prevent it from being used for criminal purposes. It is anticipated that South-East Asia will remain a significant source of safrole in the short-term, with authorities continuing to seize large quantities of safrole-rich oils throughout the region, particularly in Cambodia and Thailand. In the longer-term, both the rapidly dwindling stocks of safrole-bearing trees and stronger national controls outlawing safrole harvesting in South-East Asian countries will impact on the availability of this key MDMA precursor chemical.

DRUG ANALOGUES AND OTHER SYNTHETIC DRUGS

Drug analogues and other synthetic drugs have been present in Australia and overseas since at least the mid 2000s. These substances (such as piperazines) have typically been marketed and used as legal, but inferior, substitutes for illicit drugs such as methylamphetamine and MDMA. In recent years, however, users have increasingly sought out specific analogues to the point where a market for these has now been established.

Although the synthetic drug 4-methylmethcathinone (also known as 4-mmc, mephedrone, meow and m-cat) has received significant attention from law enforcement agencies and the media, users throughout Australia are consuming a wide range of analogues and other synthetic drugs. Many of these substances are sourced from online 'legal high' stores, legitimate fine chemical suppliers and sites selling 'research chemicals'. To circumvent law enforcement and regulations, many of these substances are marketed under the guise of incense, bath salts, room deodorisers, plant food, novelty toys, super absorbent polymer or zirconium silicate. Although ingredients may be listed, cases of intentional mislabelling have been identified, making it a more complex task to identify the active compound.

The availability of these substances and the ease with which they can be purchased over the Internet has changed the traditional user-dealer relationship and resulted in a broad supply base.

Organised crime groups currently have a limited involvement in the importation or distribution of drug analogues in Australia. The capacity of organised crime groups to develop a presence in the market depends on the degree to which personal users continue to be able to access these substances and successfully import or otherwise acquire them for personal use. While this ease of access continues, the opportunities for organised crime groups to control the market remain limited.



Apart from being used to source these drugs, the Internet also plays a significant role in diffusing information on new drug types, ways of consuming drugs, the psychoactive and negative effects of the various drug types, and drug combinations that heighten effects. The user-driven discussions also enable illicit producers to readily identify and capitalise on specific substances which are the subject of positive comment by users.

Up to 500 different 'legal highs' are advertised through online 'legal high' stores overseas, with a wide spectrum of effects such as euphoria, stimulation, altering consciousness and alleviating after-party symptoms. These highs are marketed as natural and legal and are perceived by users (in many instances, erroneously) to be less harmful than illicit drugs. Although some of these substances are legal in Australia, others are illegal or have questionable legal status yet to be tested in the courts. The extent to which the perception of legality has attracted new consumers to experiment is difficult to assess, but it has undoubtedly been a factor for some users.

The 'legal high' market, particularly in Europe, has shown high levels of innovation in production processes and marketing, with new products quickly appearing on the market when specific substances are regulated. European agencies have also identified increased marketing of stronger, more effective analogues that mimic the effects of illicit drugs. With Australian consumers purchasing analogues and other synthetic drugs online, the Australian market is likely to be affected by European trends.

The speed with which the analogue market is evolving and the vast number of potentially active compounds presents law enforcement agencies with unique challenges. These include difficulties associated with forensically identifying the compounds and ensuring that legislation is reflective of the dynamic illicit drug environment.



THE DEVELOPMENT OF SPICE

'Spice' smoking blends first appeared overseas as early as 2004 and demand for spice products increased significantly from 2008 onwards. Spice products are marketed as incense and not for human consumption, but users can purchase them as pre-rolled 'joints' or in loose-leaf form.

Before they were closely analysed, spice products were assumed to be composed of plant ingredients, with the unique blend of plant materials providing the cannabis-like effects. However, complex forensic investigations identified a range of synthetic substances that produce effects similar to cannabis. Although the source of these synthetic cannabinoids is unknown, German forensic chemists believe it was evident that the producers of these substances had gone about the process in a very methodical manner, mining the scientific literature for promising psychoactive compounds.

The substances found in spice smoking blends are obscure synthetic cannabinoids that were originally developed for research purposes. After these substances were identified, numerous countries took steps to make them illegal. According to investigations undertaken by forensic chemists in Germany, 'just four weeks after the prohibition took effect a multitude of second generation products were released onto the market. The speed of introduction of new products not only showed that the producers are well aware of the legal frameworks, but that they likely anticipated the prohibition and already had an array of replacement products on hand.'⁴³

Although organised crime groups have limited involvement in importing or distributing analogue drugs in Australia, there is an established trend, internationally and domestically, for these groups to substitute analogues and other synthetic drugs (such as piperazines) for MDMA.

As many of the substances entering the market are novel, there is limited research or knowledge about the short-term or long-term health consequences of consuming them. There is also limited information on the risk of dependence, potentially fatal doses or possible adverse interactions with other drugs. The possible role of these substances in deaths may currently be under reported because of their novel nature and the likelihood that they will not be identified through routine toxicological and post-mortem tests.

43 Lindigkeit E et al., 2009, 'Spice: A never ending story', *Forensic Science International*, 191 pp. 58–63.



HEROIN

INTERNATIONAL SITUATION

Heroin is another drug that is predominantly imported, as the incidence of locally produced 'home bake' heroin is low. As a result, international trends are vital when assessing the market. The Australian heroin market has remained generally stable over the past year. Some increases in heroin availability have been noted around Australia but these are not considered significant, with reported heroin use remaining at historically low levels.

Global potential production of opium decreased significantly in 2010 from 7245 metric tons (mt) to 4203 mt. This was due to a 48 per cent decrease in potential opium production in South West Asia (principally Afghanistan), which has historically been the largest producer of opium for the global market.

The United Nations' 2010 South-East Asia crop assessment reported that the area under opium cultivation increased 22 per cent compared with 2009, and the total potential production of opium increased 75 per cent from 345 mt to 603 mt.

Following consistent decreases in opium production in South-East Asia between 1998 and 2006, opium production in the region has almost doubled since 2006. The scale of production in South-East Asia, however, remains comparatively small when compared with the production in South-West Asia.

The re-emergence of opium production in South-East Asia, and the historical link between South-East Asian heroin and the Australian market, may result in increasing availability of heroin from this region if production continues to increase. Despite this, Afghanistan is expected to remain the primary global producer of opium for the foreseeable future. It is worth noting, however, that the vast majority of Afghani heroin is destined for Europe, Asia and North America.

DOMESTIC SITUATION

With production of opium in South East Asia continuing to rise, the availability of heroin in Australia is expected to continue to increase slowly, particularly in the major capital cities.

According to the most recent National Drug Strategy Household Survey, 11 per cent of Australians aged 14 years or older considered heroin use to be of most serious concern for the general community. This was the second-highest proportion for an identified illicit drug.⁴⁴

⁴⁴ Australian Institute of Health and Welfare, 2008, *2007 National Drug Strategy Household Survey*, Drug Statistics Series No. 20.

West African criminal groups have developed a significant presence in heroin trafficking, both globally and in Australia. They are established in primary heroin transit countries such as Pakistan, India and countries throughout South-East Asia. Individuals of Chinese and South-East Asian ethnicity also maintain a strong presence in trafficking heroin into Australia and this historical involvement in the Australian heroin market is expected to continue. Cambodia and Vietnam remain springboards for heroin trafficked from South-East Asia into Australia. Criminals of Romanian background are also long-standing suppliers to local markets.

In a study published in 2007, the estimated social costs (health effects, crime costs and road accident costs) of opiates, predominantly heroin, were A\$4.5 billion a year. The social costs of opiate use were the highest of all of the illicit drugs examined in this study (see footnote 35).

CANNABIS

The cultivation and distribution of cannabis in Australia is a large-scale, diverse and entrenched illicit market—resulting in cannabis remaining readily available. While cannabis is used across a wide range of demographic and socio-economic groups, it remains concentrated in some sections of the community.⁴⁵

Cannabis use has moderated in recent years, reflecting a trend also evident in other Western nations where consumption has stabilised or declined. According to National Drug Strategy Household Survey data, the proportion of individuals who had been offered or had the opportunity to use cannabis fell from 24 per cent in 2001 to 17 per cent in 2007.⁴⁶ Despite the moderation in use, cannabis remains the most widely used illicit drug in Australia, with an estimated 281 tonnes consumed annually.⁴⁷

The link between criminal groups and large-scale cannabis cultivation is well established. Some Australian criminal groups specialising in commercial cultivation of cannabis and historically prominent groups, including those with people of Albanian, Italian and Vietnamese background and OMCG members, remain active in the market. Some of these groups choose cannabis as their main area of illicit activity. However, the cannabis market is highly decentralised and entrepreneurial with an array of individuals and groups operating at various levels of sophistication and capacity.



⁴⁵ For example, 77 per cent of injecting drug users surveyed in the 2009 Illicit Drug Reporting Survey had used cannabis in the six months prior to interview.

⁴⁶ The decrease is even more pronounced in the 20–29 age group, which fell from 50 per cent to 38.5 per cent; Australian Institute of Health and Welfare, 2007 National Drug Strategy Household Survey: detailed findings, AIHW, Canberra.

⁴⁷ Moore, T, 2007, *Working estimates of the social costs per gram and per user for cannabis, cocaine, opiates and amphetamines*, Monograph No. 14, National Drug and Alcohol Research Centre, Sydney.

“The illicit pharmaceutical market remains largely supplied by diversion, with these drugs readily available on the illicit market from a diffuse network of suppliers, both illicit and legitimate”

No significant changes in availability or cannabis cultivation methods have been noted over the past year. Hydroponic cultivation remains the predominant form of cultivation, although large bush crops continue to be identified.

Despite the common perception that cannabis is relatively harmless, it does have a widespread impact on individuals and the general community. From 1993–2007, cannabis-related hospital separations were the third highest in number across the four drug types (after opioids and amphetamines). At a national level, these separations have steadily increased over the 14-year period covered by the data. In 2007–08, cannabis was the second most common principal drug of concern (after alcohol) for which treatment was sought, accounting for 22 per cent of episodes. When all drugs of concern are considered, 44 per cent of episodes included cannabis.

Recently published findings from long-term studies in Europe, the US and Australia have concluded that cannabis users are more likely to exhibit symptoms of psychoses including schizophrenia.⁴⁸

Cannabis continues to account for the greatest proportion of illicit drug arrests in Australia, comprising two-thirds of arrests in 2008–09. There were 55 638 cannabis arrests nationally in 2008–09, representing a six per cent increase from 2007–08. The number of cannabis arrests has remained relatively stable over the last decade. ‘Consumer’ arrests accounted for 86 per cent of cannabis arrests in 2008–09.

ILLICIT PHARMACEUTICALS

A range of legitimate pharmaceutical drugs are misused, the most common types being benzodiazepines and pharmaceutical opioids. These drugs are used for a variety of reasons, including:

- > dependence on pharmaceuticals
- > self-medication
- > withdrawal from other drugs or after using other drugs (licit or illicit)
- > to enhance the effects of other drugs by using them in combination
- > as a ‘street currency’ or for bartering.

48 Van OS, J et al, 2011, *Continued cannabis use and risk of incidence and persistence of psychotic symptoms: 10 year follow-up cohort study*, viewed 1 March 2011, <http://www.bmj.com/content/342/bmj>; Bourke, E, 2011, *Cannabis hastens onset of psychosis: researchers*, viewed 1 March 2011, www.abc.net.au/news/stories/2011/02/08; UNIS, 2011, *Early cannabis users three times more likely to have psychotic symptoms and Cannabis again linked to psychosis*, viewed 1 March 2011, <http://www.inisaustralia.com>.

Domestically, no significant changes have been identified in the illicit use of pharmaceutical drugs over the past year. A 2010 survey of injecting drug users found that:

- > 40 per cent of respondents reported use of illicit benzodiazepines
- > 46 per cent reported use of morphine
- > 32 per cent reported use of illicitly obtained Oxycodone.⁴⁹

These rates of use were comparable to previous surveys. Drug Use Monitoring in Australia data on use of benzodiazepines (licit and illicit) also shows stability in the use of benzodiazepines over the past 10 years.⁵⁰

Factors driving the pharmaceutical drug market remain unchanged. They include availability, affordability, consistency and profitability when on-sold.

The illicit pharmaceutical market remains largely supplied by diversion, with these drugs readily available on the illicit market from a diffuse network of suppliers, both illicit and legitimate.

The illicit use of pharmaceutical opioids is an ongoing problem throughout Australia, driven historically by the instability of the domestic heroin market. Although heroin availability is increasing slowly, pharmaceutical opioids remain in strong demand on the illicit market because of their ready availability and their consistent quality.



49 Stafford, J., Sindicich, N., & Burns, L. (2009), *Australian Drug Trends 2008: Findings from the Illicit Drug Reporting System (IDRS)*, National Drug and Alcohol Research Centre (NDARC), Sydney.

50 Australian Institute of Criminology, Drug Use Monitoring in Australia urinalysis data.



'PHARM' PARTIES

The US has recorded a significant increase in illicit use of prescription pharmaceutical drugs among adolescents. The term 'pharm party' has been associated with the activity where young people gather to consume prescription medicines sourced from legitimate family stocks. The phenomenon has been exaggerated and sensationalised in press reporting, potentially undermining awareness campaigns by authorities designed to curb the problem. These reports indicate that teenagers pool the tablets they had procured into 'fruit salad bowls' then proceed to consume the mixed substances in handfuls. The reports resulted in scepticism within the community that the problem actually existed, but there are continued reports of fatalities arising from uncontrolled consumption of these drugs in communal circumstances. Control measures include promoting the use of locked facilities to secure prescription medicines within the home and also programs enabling pharmaceuticals that are out-of-date or surplus to requirements to be surrendered for destruction.

'Pharm parties' have not been detected in Australia as they have been in the US. However, domestic surveys of drug use have disclosed relatively high levels of reported use of pharmaceuticals and there are close parallels between the levels of medical care in the two countries. The most recent National Drug Strategy Household Survey found that both recent use and use within a lifetime of painkillers/analgesics and tranquillisers/sleeping pills for non-medical purposes was higher than for most other illicit drugs. Australians aged 20–29 years were more likely than those in other age groups to have used pharmaceuticals for non-medical purposes in their lifetime (10.3 per cent), in the previous 12 months (5.4 per cent) and in the previous month (2.4 per cent).

Both the Australian and US systems provide sophisticated health management through a vast array of prescription medicines, with patients usually administering the drugs themselves while residing at home. The result is that a typical residence contains a significant number of drug preparations that are susceptible to illicit use. An additional factor in the adolescent use of pharmaceuticals is that the individuals consuming the substances are under the mistaken impression that these drugs are not potentially harmful because they have been prescribed by a doctor and they have seen their parents consuming the same substances, or have been given similar medication themselves, with no ill effects.

A large-scale study of the benzodiazepine and pharmaceutical opioid market in Australia⁵¹ found low levels of organised criminal activity. The ease with which pharmaceuticals can be acquired through legitimate sources limits the opportunities for organised crime groups to develop a presence in the pharmaceutical market. Available intelligence supports this assessment.

Despite the limited organised criminal involvement in this market, large-scale organised crime networks have been identified as being involved in distributing pharmaceutical drugs. The ease with which pharmaceuticals can be obtained makes this an attractive market for entrepreneurial individuals and groups.

PERFORMANCE AND IMAGE ENHANCING DRUGS

Illicit performance and image enhancing drug use has typically been associated with bodybuilders and elite athletes and, in a law enforcement context, with steroid abuse by members of outlaw motorcycle gangs and other criminal groups. However, current intelligence suggests the use of performance and image enhancing drugs is widespread. Users include members of specific occupations (such as security providers, military and law enforcement personnel), amateur sportspeople and semi-professional (as well as elite) athletes. These drugs are also used by general members of the community seeking to enhance their physique or lose weight.

Performance and image enhancing drugs are readily available through social networks of like-minded individuals, individuals within legitimate businesses such as gyms, sporting clubs and fitness centres, forged prescriptions, compliant doctors and pharmacists, thefts from medical sources (such as hospitals), the veterinary industry and Internet sales. The Internet plays an important role not only in sourcing performance and image enhancing drugs but also in providing information on their use.

Because of inconsistencies in the legal status of performance and image enhancing drugs internationally, these substances are readily available overseas and are relatively cheap compared with the illicit market price in Australia. Primary sources of performance and image enhancing drugs trafficked into Australia are Hong Kong, Thailand, Eastern Europe, the United Kingdom, India, the People's Republic of China, South Africa, the United States and Canada. The international market is sufficiently lucrative that a parallel counterfeit market is also well established.

The primary driver of the performance and image enhancing drugs market in Australia is high demand as a consequence of the large potential user base, the variety of uses, the ease of availability and the potential profitability when on-sold.



⁵¹ National Drug Law Enforcement Research Fund, 2007, *Benzodiazepine and pharmaceutical misuse and their relationship to crime: An examination of illicit prescription drug markets in Melbourne, Hobart and Darwin*, NDLERF, Canberra.



Gamma-hydroxybutyrate (GHB)

The ease with which these drugs can be obtained, and the wide user base, results in an extremely broad supply base. Although criminal individuals and groups are consistently identified as possessing and using performance and image enhancing drugs, they are just one section of the broader market. The ready availability of these drugs reduces opportunities for organised crime groups to control or have significant influence in this market.

ANAESTHETICS

GAMMA-HYDROXYBUTYRATE (GHB)

The Australian GHB (also commonly known as 'fantasy') user market remains small and stable. In 2007, only 0.1 per cent of people aged 14 years and over reported use of GHB in the previous 12 months. GHB has a range of illicit uses, including for those seeking its euphoric effects (in nightclubs or at 'raves', for example), for bodybuilding and for use as a sleeping aid. GHB users in Australia are typically young adults with extensive histories of multiple drug use.

GHB is readily manufactured from its precursors, gamma-butyrolactone and 1,4-butanediol (1,4-BD).⁵² Both gamma-butyrolactone⁵³ and 1,4-BD have legitimate applications and 1 530 228 kilograms of 1,4-BD and gamma-butyrolactone was legitimately imported into Australia between 2004 and 2009.⁵⁴ Because of inconsistencies in the regulation of gamma-butyrolactone globally, it can also be readily sourced over the Internet.

The GHB market has shown no signs of significant expansion in recent years and is expected to remain stable in the short-to medium-term.

Organised criminal groups have been implicated in the importation and distribution of gamma-butyrolactone and 1,4BD in Australia, but this appears to be instances of exploiting specific diversion opportunities or access to these substances. The capacity for users to acquire gamma-butyrolactone over the Internet for personal use will continue to inhibit organised crime groups from developing a strong presence in this market. The small size of this market also suggests that it is adequately supplied through established sourcing and distribution channels.

The use of GHB has resulted in sporadic large-scale overdoses at music events. GHB has also been described prominently in the press and electronic media as a 'date-rape' drug as it can be easily introduced into drinks, stupefying and debilitating victims.

⁵² Both GBL and 1,4-BD metabolise into GHB in the body, producing identical effects.

⁵³ Gamma-butyrolactone is an industrial solvent, used as a paint stripper, graffiti remover and alloy wheel cleaner. Gamma-butyrolactone is a prohibited import, unless imported under an import licence and a specific import permit. 1,4-BD also has various licit industrial uses.

⁵⁴ Customs and Border Protection data.

KETAMINE

The use of ketamine, like GHB, remains confined to a small proportion of the community, with 0.2 per cent of people aged 14 years and over reporting ketamine use in the previous 12 months.

The low prevalence of ketamine use in Australia is in contrast to South-East Asia, where ketamine abuse has emerged as a significant problem, particularly in the People's Republic of China and Hong Kong. According to the UN Office on Drugs and Crime, 6.3 tonnes of ketamine were seized in South-East Asia in 2008, compared with 5.2 tonnes of heroin. India and the People's Republic of China remain predominant sources of ketamine for the illicit market. The People's Republic of China is also a predominant source for legitimate ketamine.

Ketamine appears to be principally supplied through diversion from legitimate domestic sources, with some instances of attempted importations. In 2008–09 ketamine was detected 33 times at the Australian border, with 31 of these in parcel post. The total weight of detections was 7.9 kilograms, with the largest detection being 3.8 kilograms of ketamine liquid from India.

With ketamine readily available throughout South-East Asia, there is potential for it to be imported through established illicit drug trafficking routes between South-East Asia and Australia. Based on current intelligence, organised crime groups do not appear to have a significant presence in the ketamine market in Australia.

Self-reporting of ketamine use in Australia remains low. Ketamine has also historically been pressed into tablets in combination with other substances and sold as MDMA, or pressed in combination with MDMA, resulting in inadvertent use of ketamine by MDMA users. The progressive tightening of controls on ketamine, initially through scheduling by states and territories and more recently through its classification as a Prohibited Import, has restricted opportunities for its diversion. Ketamine continues to be identified in illicit tablets and drug preparations, but with reduced frequency.

The ketamine market is expected to remain a stable niche illicit market. There may be sporadic detections and appearance of ketamine on the Australian market, but sustained increases in ketamine use are not anticipated.

TRYPTAMINES

The tryptamine⁵⁵ market remains active in Australia. Lysergic acid diethylamide (LSD) can be easily concealed and detection is very difficult, because of the extremely small amounts required for an active dose (doses are commonly about 0.0001 gram or 10 000 doses per gram). Intelligence suggests that LSD is being distributed in liquid form in vials to further reduce the likelihood of detection.

⁵⁵ Tryptamines are hallucinogenic substances that act on the central nervous system, distorting mood, thought and perception. Common tryptamines consumed in Australia include LSD, psilocybin-containing mushrooms and dimethyltryptamine.



LSD powder

“The tryptamine market remains a niche market. A small sub-population uses tryptamines regularly, with the majority of users consuming them on an irregular basis, sometimes in combination with MDMA and a range of other illicit drugs”

According to National Drug Strategy Household Survey data, 0.6 per cent of individuals aged 14 years and over reported the use of hallucinogens in the previous 12 months. A much higher percentage (6.7 per cent) reported use at some time in their life, which is the third-highest percentage use of any drug after cannabis and MDMA. The pattern of tryptamine use also differs significantly from that for other drug types, with the majority of users consuming tryptamines on an irregular basis.

According to user reports, LSD is readily available in most states, with 70 per cent of users reporting LSD as either ‘easy’ or ‘very easy’ to obtain.⁵⁶ Significant discussion is also occurring in online forums on the use of LSD, psilocybin-containing mushrooms and dimethyltryptamine.

Because of the complexity of synthesising LSD, it is unlikely that it is or will be produced domestically. Hence it will continue to be sourced from established production centres overseas. There is limited intelligence on groups or individuals involved in importing LSD. Because of the comparatively small size of the LSD market and the small amount of LSD required for an active dose, significant quantities of LSD are not required to meet the demands of the Australian market.

Psilocybin-containing mushrooms and dimethyltryptamine can be acquired domestically from natural sources. As a result it is not possible to indirectly monitor the market by monitoring the diversion of chemicals. Psilocybin-containing mushrooms and dimethyltryptamine are also sold at some herbal stores.

The tryptamine market remains a niche market. A small sub-population uses tryptamines regularly, with the majority of users consuming them on an irregular basis, sometimes in combination with MDMA and a range of other illicit drugs.

⁵⁶ NDARC, 2010, *Australia Drug Trends 2010, findings from the Ecstasy and Related Drug Reporting Survey* (conference handouts), Sydney.

MARKETS FOR OTHER ILLICIT COMMODITIES

Other illicit commodities covered in this assessment are intellectual property crime (counterfeit goods) and firearms.

The counterfeit goods market is no longer confined to luxury items. Counterfeit goods range from car parts to cosmetics, and alcohol to pharmaceuticals. Apart from the losses to the businesses whose products are copied, inferior or toxic counterfeit products can harm the wider community.

While the market for illicit firearms is not as broad as the market for counterfeit goods, there is continued demand among organised crime groups and other users or collectors. An increasing number of illicit rifles and shotguns are modified to handgun specifications—the preferred weapon for firearm-related crime.

INTELLECTUAL PROPERTY CRIME: COUNTERFEIT GOODS

Intellectual property crime (IP crime) covers a range of counterfeiting and piracy offences. Counterfeiting is the illegal copying of products protected by trademarks or copyright, such as clothing and pharmaceuticals. Piracy involves the illegal copying of content such as films, music, computer games and software for profit. Counterfeiting and piracy both involve the unauthorised manufacture and distribution of these goods and works.

Overall, counterfeit goods can be divided into two main categories: digital (such as software and music) and physical (ranging from clothing to pharmaceuticals). Within both categories, counterfeit goods can be further classified into those goods that consumers know to be counterfeit and that are sold at a discounted price, and goods that are purchased at undiscounted prices in the belief they are genuine. The second category attracts greater criminal involvement and poses the greater health and safety risk to consumers, as the items—including car parts, pharmaceuticals and alcohol—may be of substandard quality.

This assessment concentrates mainly on physical counterfeit goods, reflecting the size of this market and the involvement of global organised crime. It is anticipated that future assessments will cover all aspects of IP crime including piracy and trade secrets.

Several drivers influence the importation of counterfeit goods into Australia. These include the high profit and low penalty nature of the crime market, the large potential market size, the power of genuine brands, demand, and the established distribution networks. An increasingly important driver is the ability to raise funds in this way to facilitate other crime types.



“The prevalence of counterfeit goods in this country is likely to increase in the future, driven by transnational organised crime groups capable of producing counterfeit products on an industrial scale”

The Australian Institute of Criminology observes that Australia has, by global standards, relatively low levels of IP crime. However, counterfeit goods constitute an expanding crime market in Australia. The prevalence of counterfeit goods in this country is likely to increase in the future, driven by transnational organised crime groups capable of producing counterfeit products on an industrial scale.

The Organisation for Economic Cooperation and Development (OECD) has noted the expanding scope of products being counterfeited globally, with a notable shift from high-value luxury items to common products. This is reflected in Australia, where the range of counterfeit items seized by Customs and Border Protection now includes car parts, alcohol, cosmetics, laundry powder and batteries, as well as traditional items such as textiles and clothing. Nevertheless, luxury items remain part of the counterfeit market. The increase in counterfeiting of common products also increases the risk of physical harm to consumers, as this includes items that are ingested, used for hygiene or connected to household appliances and electricity grids.

The range of pharmaceuticals counterfeited globally is broadening from lifestyle drugs to items for treating heart conditions and cancer. It is unclear if this trend is reflected in Australia, although Australia’s Pharmaceutical Benefits Scheme has probably reduced the domestic demand for counterfeit pharmaceuticals. However, global seizures of counterfeit pharmaceuticals rose by 700 per cent in 2008. Although seizures in Australia are low, this indicates an increased potential threat. It is possible that this growth in counterfeit pharmaceuticals is linked to the equally rapid appearance of unregulated ‘online pharmacies’ on the Internet, selling prescription pharmaceuticals.

Rapid increases in technology will facilitate IP crime. IP theft will pose increasing challenges for both private and government interests, which could lead to the sale of confidential and sensitive information on the global market. The theft and use of ‘information’ is already occurring and is likely to increase as advanced countries transform into information-based economies. An international survey of 800 companies⁵⁷ conducted by researchers from Purdue University, Indiana for McAfee Inc. identified that, in 2008, the surveyed companies estimated they lost a combined US\$4.6 billion worth of IP and spent US\$600 million repairing damage from data breaches. Based on the survey results, McAfee Inc. estimated that companies world-wide suffered IP-related losses of more than US\$1 trillion during 2008.⁵⁸

⁵⁷ Center for Education and Research in Information Assurance and Security, 2009, *Unsecured economies: protecting vital information study*, Purdue University, Indiana.

⁵⁸ Australian Security Magazine, *Intellectual property protection*, Issue No. 42 – 2009, p.1

Computer circuitry is also being counterfeited globally and some of the counterfeit circuitry is being unintentionally used in military and other government systems around the world. The use of malicious programs such as rogue antivirus or pirated copies of computer operating systems may leave the user vulnerable to the compromise of sensitive personal and corporate information or lead to the unlawful use of the victim's computer in the facilitation of other criminal activities. In late 2009, coordinated cyberattacks were directed at US computer networks with the alleged intention of stealing IP to gain competitive advantage in the global economy for companies linked to the perpetrators. Australian companies are not immune to this threat.

The People's Republic of China continues to be the dominant source country for counterfeit goods in Australia, with 80 per cent of goods seized originating there. India and South Korea are becoming more significant as source countries, accounting for six per cent and five per cent of seized items respectively, according to Customs and Border Protection information. This reflects global trends, with Asian countries identified as the main originating countries.

Counterfeit products are increasingly being sold through legitimate retail shops, creating greater exposure to risk for unknowing consumers.

Globally, organised crime groups are increasingly involved in intellectual property crime, in particular counterfeit goods trafficking. Members of outlaw motorcycle gangs and Italian organised crime groups have been identified as being involved in importing counterfeit goods into Australia, but the involvement of organised crime groups is likely to be more diverse. Middle Eastern and Asian organised crime groups are known to be prominent in specific areas within the counterfeit goods market globally. Given the known presence in Australia of these groups, it is probable that they do, or will in the future, have some involvement in the domestic counterfeit goods market.

The harm associated with counterfeit goods arises from a number of factors. It is a disincentive for innovation, as companies are less inclined to invest in research and development if products are quickly counterfeited. Other harms include the substantial illicit proceeds which are derived and which may be channelled to criminal networks, organised crime and other groups that disrupt and corrupt society. In addition, business is harmed by decreased sales and licensing proceeds. Reputations and brand names of genuine products are damaged, causing financial losses for the manufacturer. Consumer safety is also a pressing concern, given the potential for serious injury or death from inferior or toxic products.

“Globally, organised crime groups are increasingly involved in intellectual property crime, in particular counterfeit goods trafficking”





FIREARMS

In Australia there is continued demand for illicit firearms by organised crime groups, criminals generally and certain firearms enthusiasts. Criminal use of firearms is an enabler, used to protect interests and commit acts of violence. Firearms trafficking—the sale and movement of illicit firearms—is one of the organised crime types capable of generating illicit funds, albeit on a smaller scale than other enablers.

Organised crime groups have been known to access illicit firearms predominantly through corrupt licensed dealers, loose networks of criminal gangs with access to firearms and 'backyard' manufacturers. Most illicit firearms seized appear to be commercially manufactured. An increasing number of illicit rifles and shotguns have been modified to handgun specifications. Handguns tend to be the preferred weapon in firearm-related crime. They make up the largest single category of all firearm types traced by the ACC and also represent the largest category of firearm with serial numbers defaced. Burglaries of dealers and firearm holders represent a relatively small source; Australian Institute of Criminology research during the last five years indicates that handguns are the type of firearm stolen least often in Australia. This suggests that there are sufficient handguns already in circulation to meet demand.

CRIMES IN THE MAINSTREAM ECONOMY

These crime markets have particularly widespread ramifications for the community.

Whether it is dealing with credit card fraud, losing savings in a dubious investment scheme, being lured by an early-release superannuation scheme or stung by a mass marketing email scam, crimes in the mainstream economy ultimately hit the hip pocket of many individuals and businesses alike.

INSURANCE FRAUD

Insurance fraud is the deliberate falsification of material by an insurance claimant to obtain a financial advantage or gain. Insurance fraud ranges from individuals overstating the value of damaged or lost items, or not declaring information that is known and relevant to a claim, through to the activities of highly organised criminals coordinating large and complex false claims.

Most insurance fraud relates to false or overvalued claims by individuals. More specialised insurance fraud includes false workers' compensation and personal injury claims, staged accidents, organised theft, fire and property damage, and fraud instigated by companies or company employees.

The Australian insurance industry represents one of the largest commercial sectors within the country. It generated in excess of A\$25.3 billion in revenue in 2009 and incurred claims to the value of A\$14.8 billion.

The insurance sector has one of the highest reported rates of economic crime. This is partly the result of robust and proactive anti-fraud measures, which are effective in detecting fraud. Insurance fraud typically relates to high-volume, low-value claims. Improved information sharing within the insurance industry has helped detect organised criminal involvement in insurance fraud, particularly cross-company fraud.

In the UK, the Serious Organised Crime Agency reports that organised criminals are suspected of carrying out approximately 12 per cent of insurance fraud, particularly motor insurance fraud. The use of staged accidents by organised crime groups also continues in Australia. Some crime groups are carrying out staged accidents and submitting multiple claims for the same loss. Fraudulent personal injury claims provide crime groups with the opportunity to generate funds. In some cases, fraudulent personal injury claims may be submitted in conjunction with staged accidents to maximise income. Multiple fraudulent claims are likely to be made with separate insurers to minimise the risks of detection.

Some criminal groups engaged in insurance fraud exhibit high levels of sophistication and organisation. Examples include criminals adapting their modus operandi to avoid or counter industry profiling and fraud detection methodologies, exporting stolen vehicles to nations in the South Pacific region for resale and using 'hibernation periods' between purchasing vehicles and subsequently involving them in staged accidents. Although the majority of organised criminal involvement in insurance fraud relates to motor vehicle insurance fraud, fraud related to marine craft and construction equipment is an emerging problem.

SUPERANNUATION FRAUD

Superannuation fraud is defined as an intentional misstatement of information to obtain financial benefits from superannuation through improper, unauthorised or illegal action. Types of fraud committed in the superannuation industry include illegal early release schemes (see below), diversion of funds, theft of benefits by one trustee from another, misappropriation of assets and using false identity documents to access the superannuation savings of a beneficiary without their knowledge.





Superannuation holdings are a major element of the Australian financial system, with holdings at the end of 2009 totalling about A\$1.23 trillion. Australia's superannuation system is expected to grow strongly over the coming 15 years, underpinned by mandatory contributions and demographic factors. The size of Australia's superannuation holdings is expected to reach A\$3.2 trillion by 2025.

The superannuation industry is highly regulated. Fraudulent access to funds requires fraudulent identification, false statements, professional facilitation or complicit staff with approval and verification permissions within companies. Examples of criminal activity in the superannuation sector have been identified and there is potential for this activity to increase, despite the level of regulation and enforcement.

Criminal activity in this context generally involves one of two scenarios:

- > Illegal early release schemes whereby a promoter puts in place a mechanism (for example, establishes a self managed superannuation fund) to facilitate the rollover of superannuation from a client's existing superannuation fund—the outcome is that the promoter receives a fee from the client and the client obtains illegal early access to the funds.
- > Illegal early access to funds whereby a beneficiary of a superannuation fund gains access to their own superannuation savings before they are legally entitled to do so, by fraudulent means.

The majority of superannuation fraud happens at an individual level, with people using false declarations and documents or abusing their responsibilities to facilitate early access to superannuation holdings. An example of the first category of this type of superannuation fraud is a beneficiary fabricating hardship grounds to access funds. An example of the second category is a trustee of a self managed superannuation fund using fund monies to meet payments on their personal debts or for other personal expenses, in circumstances where they are not legally entitled to do so.

However, more organised early-release schemes continue to be promoted by self-managed superannuation funds administrators, tax agents, accountants, financial planners and investment advisers. These schemes are relatively unsophisticated but can result in significant loss to the superannuant.

Identity theft and false identities remain the key enablers of superannuation fraud, particularly frauds involving criminal access to an unwitting beneficiary's superannuation account. Fraudulent identities may also be used to attempt to access unclaimed superannuation, which was estimated to total A\$12.9 billion as at 30 June 2008.

There were 416 145 self-managed superannuation funds at the end of 2009, accounting for 30.9 per cent of assets across various fund types and 99 per cent of the total number of superannuation funds. About 2500 self-managed superannuation funds are established each month.

While all fund trustees have a responsibility to detect or prevent fraud, in the case of self-managed superannuation funds the responsibility is placed on trustees who may be inexperienced, poorly trained and unqualified to perform the role and, sometimes, complicit in the fraud, making these funds particularly vulnerable to exploitation by negligent or disreputable trustees or professional service providers.

SUPERANNUATION EARLY-RELEASE SCHEME

A network of individuals established an unlicensed financial services business that offered clients early access to their superannuation funds. This business acted as a trustee for a self-managed superannuation fund. It is alleged that the preserved superannuation benefits of 121 clients, worth more than A\$3.5 million, were deposited into the self-managed superannuation fund's bank accounts (in and of itself this breached the rules governing the establishment of self managed superannuation funds, which place a strict limit on the number of fund members). These funds were rolled over from 11 legitimate superannuation funds. The self-managed superannuation fund managers then allegedly obtained early access to these benefits, withdrew the funds and distributed them to the clients. As part of this process the fund managers retained commissions totalling more than A\$685 000 from the clients' funds. The suspects subsequently transferred the commissions out of Australia through a series of low-value international funds transfers to the Philippines and Pacific Island nations.

In seeking to enhance the integrity of Australia's superannuation system, the recently finalised Review into the Governance, Efficiency, Structure and Operation of Australia's Superannuation System (the Cooper Review) focused particular attention on the self-managed superannuation funds component of the sector and early-release schemes. The principal recommendations of the review relating to these matters were:

- > Introducing legislation to require proof of identity checks for all people joining a new or existing self-managed superannuation fund. These checks will not be retrospective unless an existing self-managed superannuation fund is organising a rollover from a large Australian Prudential Regulation Authority (APRA) fund.⁵⁹ In these instances verification checks will be conducted.

⁵⁹ APRA supervises regulated superannuation funds, other than self managed superannuation funds (these are supervised by the Australian Taxation Office), and Approved Deposit Funds and Pooled Superannuation Trusts.



- > Introducing a system to enable large APRA funds to verify the details of self-managed superannuation fund membership, including the use of tax file numbers, before processing rollover requests.
- > Introducing controls around the naming of self-managed superannuation funds to reduce the current ability for them to have similar names to large APRA funds.
- > Introducing enhanced resources for self-managed superannuation fund trustees to enable these individuals to carry out their trustee responsibilities more competently.
- > Amending legislation to prohibit the acquisition of collectables and personal use assets (such as wine, exotic cars and jewellery) by self-managed superannuation funds.⁶⁰
- > Amending legislation so that rollovers to a self-managed superannuation fund are captured as a designated service under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cwlth)*.

In addition, during 2010 the Australian Taxation Office introduced new measures to combat illegal early release schemes. Under the new arrangements, APRA regulated superannuation funds can now check with the Australian Taxation Office to determine whether a fund member who is requesting a rollover of funds to a self managed superannuation fund is actually a member of that self managed fund.

The structure and regulation of the superannuation industry in Australia restricts the ability of organised crime groups to target major superannuation funds, but this has not stopped such activity from occurring. Although most superannuation fraud is committed by opportunistic individuals, evidence has emerged of groups specifically targeting superannuation holdings.

CARD FRAUD

Card fraud is defined as the fraudulent acquisition and/or use of debit and credit cards for financial gain. Card fraud may involve the acquisition of legitimate cards from financial institutions using false supporting documentation (application fraud) or stealing legitimate credit and debit cards before the designated customers receive them. It may also involve phishing,⁶¹ card-not-present fraud, creating false identity documents to support a false card transaction, hacking into company databases to steal customer financial data and card skimming.

⁶⁰ This recommendation was not supported by the Australian Government.

⁶¹ Phishing refers to attempts to obtain sensitive personal and banking information (such as bank account numbers, passwords and credit card numbers) for illicit financial gain.

Card transactions have continued to increase substantially over the past decade. For example, during that period credit card transactions have increased from 42.8 million to 118.8 million per month. Australians spend A\$17.8 billion per month on credit cards and A\$11.3 billion per month on EFTPOS transactions, and they withdraw A\$12.4 billion per month from ATMs.

Skimming devices continue to be attached to some ATMs in Australia. As well, a recent shift has been observed in organised crime group behaviour, from a focus on ATM card skimming towards skimming from EFTPOS terminals.

Australia is currently working towards the universal introduction of chip and PIN technology by 2013. Although this is expected to be effective in reducing physical card transaction fraud such as skimming, it is likely that there will be some displacement towards other types of card fraud. For example, card-not-present fraud is likely to increase.

Australian and transnational organised crime groups are known to be involved in card fraud. Several organised crime groups have recently been identified as being involved in large-scale card skimming in Australia. These groups, mainly from Romania, South-East Asia and Sri Lanka, may be involved in either skimming card data in Australia and withdrawing cash overseas, or skimming data overseas and withdrawing cash in Australia.

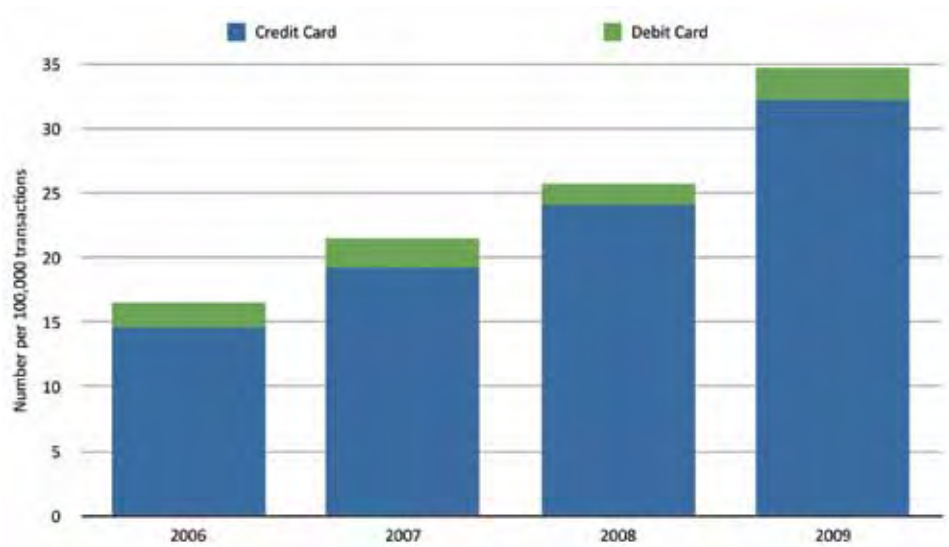
Organised crime groups have recruited financially vulnerable individuals to participate in shopping holidays to Australia, using fraudulent or stolen credit cards. These groups look to purchase high-value goods such as electronics and jewellery. By recruiting shoppers, organised crime groups involved in card and identity fraud distance themselves from fraudulent card use.

“Australian and transnational organised crime groups are known to be involved in card fraud. Several organised crime groups have recently been identified as being involved in large-scale card skimming in Australia”

If chip and PIN technology proves effective, organised crime groups involved in skimming are likely to shift their operations to countries where such technology has not been implemented. Organised crime groups are also likely to investigate methods of bypassing chip and PIN technology.

Credit card fraud has continued to increase substantially, growing by more than 200 per cent over the past three years (see Figure on page 82).

FRAUD AS OCCURRENCE PER 100,000 TRANSACTIONS



Card-not-present fraud increased by approximately 25 per cent for the 12 month period to June 2009. Card fraud is estimated to have cost Australia A\$147 million during 2009, a slight increase over the 2008 loss of A\$144.7 million. Significantly, card-not-present fraud increased in international markets when chip and PIN technology was implemented. This is expected to be mirrored in Australia after the universal implementation of chip and PIN technology by 2013.

The greatest loss from card fraud is generated by card-not-present fraud, followed by counterfeit or altered cards, lost or stolen credit cards and fraudulent applications.

There is good data sharing about card fraud between financial institutions and law enforcement. More than 657 000 cases of card fraud on Australian issued credit and debit cards were reported in Australia during 2009. The value of credit card fraud was estimated at 57.15 cents per \$1000 transacted in 2009. The value of debit card fraud during that year was estimated at 9.43 cents per \$1000 transacted. These fraud costs are low compared with other developed economies. For example, the UK credit card fraud rate is \$1.18 per A\$1000 equivalent.⁶²

⁶² APCA, *Payment Fraud Statistics – Summary of Results*, Sydney 2010 and APCA Media Release, *Payments fraud in Australia: mixed results*, Sydney, 7 June 2010.

TELECOMMUNICATIONS FRAUD

Telecommunications fraud is the use of telecommunications products or services with no intention of payment. Although communications operators have increased measures to minimise fraud and reduce their losses, criminals continue to exploit communications networks and services. More than 200 variants of telecommunications fraud exist. Globally, the top fraud loss categories are subscription fraud (about US\$22 billion per year), compromised Public Automatic Branch Exchange (PABX) voicemail systems (about US\$15 billion per year) and premium rate service fraud (about US\$4.5 billion per year).

Within the Australian telecommunications industry, post-paid mobile subscription fraud is the most dominant category (over A\$18.6 million per year), followed by Internet services (about A\$10 million per year), pre-paid mobile subscription fraud (about A\$4.4 million per year) and exploitation of fixed-line services (about A\$2 million per year). The most common forms of telecommunications fraud involve using fictitious identities to acquire mobile and landline communication products and services.

Widespread uptake of 'mobile wallet' or 'e-purse' systems may provide opportunities for fraud. Over 50 million individuals in the US are expected to be using mobile devices for banking functions by 2013.

Opportunities exist for organised crime groups to engage in PABX fraud (illegally hacking into companies' IT systems to gain free access to telephone services). Despite the potential for significant profits, PABX fraud is dominated by overseas-based organised crime groups, with Australia largely a victim country. Although the cost of most telecommunications fraud is absorbed by providers, the liability associated with PABX fraud remains with customers.

US\$55 MILLION MULTI-JURISDICTIONAL PABX FRAUD

In 2009, three Filipino residents of the US were accused of committing large-scale PABX fraud that resulted in the sale of 12 million minutes worth of call time, valued at more than US\$55 million. The three individuals were accused of hacking into PABX systems owned by more than 2500 companies in the US, Canada, Australia and Europe between 2005 and 2008. They sold access to the compromised networks to call centres in Italy for about US\$100 per network. The Italian call centres were allegedly financed by five Pakistani nationals, who were subsequently arrested by Italian authorities. The Filipino defendants have been charged in the US with computer hacking, conspiracy to commit wire fraud and access device fraud.



INVESTMENT FRAUD

Investment fraud is a generic term that incorporates a range of conduct such as securities and share market fraud, mortgage and other loan fraud and other fraudulent schemes such as Internet-based fraud and Ponzi schemes.

Regulations and controls are extensive within the finance sector, but the diversity of the sector creates numerous opportunities for criminals to generate large profits.

The use of company structures and legitimate business processes to facilitate and disguise fraudulent investment activity is crucial for many investment and financial services frauds.

SECURITIES AND SHARE MARKET FRAUD

Law enforcement has historically focused on the use of the financial market to launder or conceal proceeds of crime. More recently, law enforcement and the Australian Securities and Investments Commission (ASIC) have focused on criminal exploitation of the market and its participants through artificial manipulation of the price of equities for personal gain.

There is limited evidence of organised criminal involvement in fraud and money laundering within the Australian financial securities industry. Most current criminal activity involves low-level fraud committed by individuals against participants in the industry.

Serious criminal activity within the industry (mostly comprising smaller-scale criminal acts) is likely to continue and may increase. However, a large-scale and potentially crippling organised criminal threat to the financial securities industry is not likely while alternative, more attractive opportunities for fraud and money laundering remain available.

MORTGAGE AND LOAN FRAUD

Mortgage fraud facilitated through brokers has been identified across various financial sectors. A significant proportion of mortgage fraud originates through the mortgage broker network. Brokers have facilitated mortgage fraud by exploiting valuation thresholds, failing to comply with identity proof standards, colluding in the production of or ignoring fraudulent documents and colluding with mortgage coordinators to facilitate loans for co-conspirators.

FRAUDULENT INVESTMENT SCHEMES

Ponzi schemes are a prominent form of fraudulent investment scheme. Other examples of these schemes use deceptive marketing to secure clients for services that ultimately attract higher costs than advertised.

Ponzi schemes may be fraudulent from inception, or may start as a legitimate business but evolve into fraud at a later stage when the legitimate business fails to produce adequate returns. Ponzi scheme promoters typically have backgrounds in finance and some may have had previous involvement in fraud. A high-profile international example is the Bernard Madoff case; as described on page 23, his scheme operated in the US for many years and resulted in investors losing more than US\$65 billion.

There is potential for investment fraud to extend into 'virtual worlds' such as Second Life. In 2007, about US\$75 000 was lost when a bank in Second Life collapsed after offering 40 per cent interest per year on virtual currency investments. This virtual Ponzi scheme was able to operate without any regulatory scrutiny; it demonstrates the potential that virtual worlds offer for financial fraud to be carried out in the absence of any external regulatory oversight.

A common form of investment fraud is 'boiler-room' fraud. Boiler-room fraud, which has been detected in Australia, involves the illegal and/or aggressive selling of worthless or overpriced shares or those traded in limited volumes or markets. Boiler-room fraud is generally highly organised, spanning multiple jurisdictions and encompassing the use of sophisticated technology and identity fraud. UK investors reportedly lose at least 200 million pounds a year from boiler-room fraud perpetrated by organised crime groups. Losses in Australia are in the millions of dollars.

Both opportunistic criminals and established organised crime groups have an ongoing and established presence in investment and financial services fraud. The breadth and depth of infiltration of this sector by established and extensive organised criminal networks appears to be increasing.

Investment and financial services frauds are commonly linked to other criminal offences such as money laundering, tax evasion, corruption, coercion and intimidation, document fraud and identity crime.

SECURITIES AND SHARE MARKET FRAUD

Individual participation in the Australian share market is relatively high, with about 51 per cent of the Australian population identified as shareholders. A major event driving down the stock market could seriously impair the financial security of a great number of Australians, particularly those approaching retirement. A significant percentage of the value of managed funds and superannuation is tied to the wellbeing and continuing prosperity of financial markets. Examples of fraud and criminal behaviour in this segment of the market include people purporting to continue trading while companies are insolvent, failure to disclose the true position of companies to shareholders and failure to make full and honest disclosures to potential shareholders in a prospectus.

ADVANCE FEE FRAUD

Advance fee fraud is defined as any fraud requiring a victim to make payment/s in advance of the promised receipt of a large monetary or other material benefit. The extent of advance fee fraud in Australia has continually increased over the past five years. There has been a recent increase in the number of advance fee fraud variations observed in Australia, with inheritance, lottery, romance and employment frauds increasing.

Although advance fee fraud has traditionally been conducted by individuals in West Africa (particularly Nigeria), the last few years have seen this type of fraud emanating from a growing number of countries worldwide, predominantly within Europe and North America. In the near future, international syndicates involved in advance fee fraud are likely to increasingly target new markets in Asia, where large populations and increasing affluence combine to offer the potential for high profits. However, Nigerian nationals are still responsible for most advance fee fraud.

Organised crime groups are drawn to forms of mass marketing fraud such as advance fee fraud because of the vast profit potential and, in some cases, the capacity to fund other criminal activities. The nature and the extent of organised crime group involvement varies. Some groups are fully involved in the schemes from start to finish, while others may only provide support services such as mailing and payment processing, web hosting for fraud-related Internet sites and fraudulent identification documents.

The size, sophistication and organisation of foreign-based entities involved in advance fee fraud have increased. Some groups exploit highly complex psychological triggers to target victims. International syndicates are also showing increasing signs of combining advance fee fraud with other offences such as identity crime, counterfeiting and, in some cases, drug trafficking.

There is little evidence that Australian-based organised crime groups are involved in advance fee fraud, but isolated cases of individual involvement have been identified. This has largely related to providing support services for overseas-based syndicates.

It is difficult to accurately assess the total losses caused by advance fee fraud. Victim reporting is limited because of the embarrassment (and, in some cases, fear) attached to reporting such activity. Advance fee fraud losses by companies and individuals in Australia are likely to be hundreds of millions of dollars. Globally, victims of advance fee fraud lost an estimated US\$9.3 billion in 2009, which is an increase from an estimated US\$6.3 billion in 2008. The top three countries for advance fee fraud losses in 2009 were the US (US\$2.1 billion), the UK (US\$1.2 billion) and the People's Republic of China (US\$936 million).⁶³

⁶³ Ultrascan Advanced Global Investigations, 2010, '419 Advance fee fraud statistics 2009', 28 January 2010.

WELFARE FRAUD

Welfare fraud refers to the intentional misuse of welfare systems by withholding information or providing false or inaccurate information to obtain illegitimate welfare payments and benefits. During 2009–10, Centrelink distributed A\$84.2 billion in social security payments to 7.02 million customers.

Non-compliance represents the majority of Centrelink's overall customer debt, with fraud present in only a small percentage of cases. The majority of welfare fraud is individual and opportunistic.

Identity crime will continue to drive welfare fraud, even though data matching is providing better identification of high-risk customers.

Natural disasters and emergencies such as the 2009 Victorian bushfires, the 2011 floods and Cyclone Yasi required a reallocation of Centrelink resources to help those in need. In these cases, reduced identity verification standards are sometimes needed so that payments can be delivered quickly. Preventative processes to cross check claim data continue to improve compliance at the time of granting payments. Post-event profiling and investigations by Centrelink have also identified individuals exploiting these lowered identity requirements to fraudulently claim welfare payments. After the Victorian bushfires, over 300 instances of fraud were identified from approximately 53 000 claims made.

EXPLOITATION OF EMERGENCY RELIEF PAYMENTS

An individual living in a north Melbourne suburb contacted Centrelink 28 times during February and March 2009 to claim the A\$1000 Australian Government disaster recovery payment after claiming his house had burnt down. Each time, the individual provided a false name, date of birth and address. The individual obtained a total of A\$28 000 in benefits, Centrelink post grant profiling detected this offender, who was given a 30 month jail sentence with a 15 month non-parole period.

The cash economy has been identified by a number of Government agencies as an ongoing area of risk. Industries involved in the cash economy use business practices that are vulnerable to exploitation, such as cash-in-hand payments. Industries identified as being particularly vulnerable are building and construction, hotels and clubs, motor vehicle retailers, restaurants, taxis, hairdressers, cleaning services, the commercial fishing industry, harvesting and fruit-picking.



It is difficult to ascertain the nature and extent of organised criminal involvement in welfare fraud although the ACC is collaborating with Centrelink and other agencies to shed light on this. The 2010–11 Federal Budget allocated A\$71 million over four years to provide Centrelink with an ongoing capability to use information from intelligence and law enforcement agencies to investigate people suspected of engaging in welfare fraud, particularly in the context of organised crime. The government estimates this initiative will save more than A\$127 million over the four years.

REVENUE AND TAXATION FRAUD

The Australian Taxation Office uses a generic definition of fraud to cover revenue and taxation fraud. Fraud is defined as dishonestly obtaining a benefit, both tangible and intangible, by deception or other means.

In 2008–09, the Australian Taxation Office collected A\$264.5 billion. Income tax is the largest source of federal revenue, accounting for approximately 75 per cent of total revenue collection, followed by goods and services tax (GST) at 15 per cent and excise on alcohol, tobacco and petroleum, which accounts for about 10 per cent.

Intelligence suggests that organised crime groups are having an increasing impact on the taxation system by exploiting a range of areas such as refund fraud, illicit tobacco and offshore tax arrangements to conceal income or falsify deductions.

Organised crime groups mainly exploit the GST system to ensure or increase the profitability of otherwise legitimate businesses. Specific examples are:

- > concealing luxury motor vehicle transfers to known criminals
- > adopting false identities to facilitate lodging fraudulent business activity statements
- > exploiting the cash economy and unlawful business practices within the private security industry (this is widespread in this industry and includes not lodging business activity statements and income tax returns and understating business income)
- > defrauding the GST system through false invoicing in property development projects
- > diverting excisable goods held for export to the domestic market, to avoid both excise and GST.

Organised crime has also been identified as engaging in excise fraud. This may involve criminal exploitation of fuel tax credits, fuel substitution and the importation and trade of illegal tobacco.

Organised crime groups are increasingly using a sophisticated network of businesses, proprietary companies, partnerships and/or trusts to facilitate criminal activities and launder significant amounts of cash acquired as a result of those activities. This requires organised crime business operators to engage professional financial advisers to manage their financial affairs.

Online gambling is an identified money laundering risk and increasingly is also acknowledged as a risk for revenue and taxation fraud. This is because of the difficulties associated with identifying the source of income and the actual geographic location where the gambling activity takes place. Australia exhibits relatively high levels of gambling, with Internet gambling increasing by approximately 11.8 per cent between 2001 and 2005.

Organised criminals are represented in a variety of industries, including being second-hand motor vehicle dealers, building and construction contractors and tow truck operators and operating carwash facilities, private security entities, transport, entertainment venues, tattoo parlours and earthmoving equipment. These businesses may provide opportunities to manipulate various Australian Taxation Office products and systems. Reported income may be either non-existent or minimal and business activity statements are frequently not lodged.

As at 31 December 2010, the multi-agency Project Wickenby has raised additional tax assessments totalling \$988.93 million, recouped \$238.25 million in tax, achieved a compliance dividend of \$301.70 million and collected \$2.1 million in other moneys—resulting in a total collection of \$542.05 million. The agencies involved in Project Wickenby are also deterring people who were likely to evade tax.

When organised crime groups participate in legitimate industries, it places pressure on legitimate businesses to compete on the same distorted basis. For example, criminal activities such as tax evasion give criminal groups a competitive advantage over legitimate operators in the same industry. This may subsequently result in legitimate operators adopting poor compliance behaviours to remain competitive, further undermining the integrity of the tax system. It may also force legitimate businesses out of the industry, leaving a situation where market forces no longer dictate the cost of services.

ILLEGAL TOBACCO

Most illicit tobacco is imported into Australia. However, there have been three significant seizures of locally produced tobacco since the closure of the legal Australian tobacco growing industry in October 2006. The expertise and infrastructure for growing and curing tobacco still exists in Australia and all seizures of locally produced tobacco are suspected to be linked to former licensed growers.



Dried tobacco



In July 2009 the Australian Taxation Office executed *Excise Act 1901* search and seizure warrants on properties in New South Wales. The properties were linked to people with a history of involvement in the illicit tobacco trade. Infrastructure such as hothouses and irrigation systems, usually associated with the cultivation of market garden vegetables, had been used to grow a sizeable crop of illicit tobacco. This was the first time the Australian Taxation Office had seen hothouses used for illicit tobacco cultivation and the first time this had been detected in that particular region of New South Wales, which was well outside the traditional growing areas of north-eastern Victoria and far north Queensland. Recent intelligence suggests further illicit crops are being grown and cured in New South Wales and Victoria, including in non-traditional growing areas.

It is likely that molasses tobacco is also being illegally manufactured in Australia—in at least one city it is being sold at a price that does not appear to include excise or customs duty. Customs and Border Protection import information reveals a trend of imports of the various ingredients used to manufacture this product. It is possible that illicit manufacture is taking place using duty-paid roll-your-own tobacco or illicit tobacco products.

Organised crime networks have been linked to the importation of counterfeit brands of cigarettes and loose tobacco. The successful interdiction of illicit tobacco products at the border, the high illicit profits and increases in the excise duty on tobacco products are likely to increasingly attract organised crime groups to the illicit tobacco market through domestic cultivation and distribution.

Illicit tobacco and cigarettes are primarily distributed through small legitimate retail outlets or market stalls. As the tobacco plant leaf has not been appropriately processed and treated, it can contain dangerous contaminants such as insects, fungi, soil and pathogens.

It is reported that significant government revenue is lost through the activities of groups involved in illicit tobacco importation and illicit growing, curing, manufacture and sale of tobacco products. According to the only available source,⁶⁴ modelling results suggested that more than 12 per cent of all tobacco consumed in Australia is illegal and escapes excise. It was also estimated that 2.3 million kilograms of illegal tobacco was consumed in 2009, costing the Australian Government more than A\$600 million in lost revenue.

⁶⁴ PricewaterhouseCoopers, 2010, *Australia's illegal tobacco market, counting the cost of Australia's black market*.

HEALTH FRAUD

The health sector comprises approximately A\$70 billion of Commonwealth and state/territory budgets per year. Medicare, PBS and rebate schemes account for A\$18 billion per year.

Criminal behaviour in the health sector is largely high-volume, low-level non-compliance and fraud. Fraud represents only a small proportion of total non-compliance.

An increasing demand for health services is being driven by an ageing population, advances in medical technology and the Australian Government's desire to prevent and treat emerging lifestyle diseases. The last 10 years have seen significant growth in the number of providers of Medicare Australia services, the total number of services claimed, the number of Medicare Benefits Schedule items and the level of expenditure. This growth necessarily increases exposure to losses through non-compliance.

Non-compliance and fraud are most likely to involve false claims for services provided, false claims for services not provided, subsidised medical services for those not entitled and the misrepresentation of concession entitlements.

There are intelligence gaps around the presence and intent of organised criminal activity in the health sector, and criminal involvement with healthcare providers and practitioners.

Health fraud generally involves professionals working within the industry and individuals external to the industry. There is little corroborated evidence of systemic attack by organised crime groups external to the sector.

There are few major cases of fraud against Medicare Australia and the PBS. Most activity is committed by individuals or small groups. Some criminals are selling fraudulent Medicare cards and optical products. There are also organised sales of misappropriated prescription drugs.

In 2008–09, Medicare Australia made three confiscations of PBS medicines at airports and international mail exchanges. This indicates that individuals have obtained subsidised pharmaceuticals under the PBS and attempted to export these products, most likely for subsequent resale.

International trends suggest more organised criminal activity in the health sector is probable in the future.

In the US, Russian crime groups are involved in health fraud, driven by multiple points of vulnerability, the low risk of detection within a huge sector and perceptions of lenient punishment. If domestic crime groups seek to increase their involvement in health fraud as healthcare expenditure grows, Medicare Australia and the PBS are likely to be targeted. That said, Medicare Australia devotes significant time and resources to detecting non-compliance and fraud.





CRIMES AGAINST THE PERSON

Australian industries exploited by people traffickers include the recreation, hospitality, agricultural, construction, domestic services and sex industries.

People smugglers also target Australian borders, with a significant increase in irregular maritime arrivals since September 2008.

PEOPLE TRAFFICKING

People trafficking is the physical movement of people domestically or across borders through deceptive means, coercion or force. The US Department of State estimates that 800,000 people are trafficked across borders globally each year, 80 per cent of whom are adult females or children. These figures are conservative and exclude the millions of victims trafficked within national borders. Men, women and children are trafficked for a wide range of purposes, including sexual servitude, forced labour, the harvesting of body organs and illicit adoption.

Opportunities to traffic people into Australia are limited because of our strong migration controls and geographic isolation. However, Australia is a destination country for victims of trafficking, mainly from Asia. The majority of victims identified by Australian authorities have been women working in the sex industry (in both legal and illegal brothels). However, authorities are increasingly identifying people who have been trafficked for exploitation in other industry sectors including hospitality, agriculture, construction, domestic services and recreation. Most victims of trafficking who have come to the attention of authorities have been in Sydney and Melbourne, which may reflect the population concentration and the size of the local sex industries in those cities. It is possible that people trafficking also occurs in other parts of Australia, albeit on a smaller scale, which makes it more difficult to detect. Police investigations also reveal that victims are frequently moved around the country, especially between the mainland state capitals.

In Australia, cases of trafficking for sexual exploitation have largely involved small crime groups, rather than large organised crime groups. The small crime groups use family or business contacts overseas to facilitate recruitment, movement and visa fraud. People trafficking matters have also generally involved other crime types, including immigration fraud, identity fraud, document fraud and money laundering.

People trafficking offenders are sophisticated, and flexible enough to adapt to law enforcement activity, prosecutorial strategies and changes in migration regulations. People trafficking investigations have revealed changes in the techniques used by traffickers and in the conditions experienced by their victims. For example, investigations suggest that it is increasingly unusual for a victim of trafficking to be physically restrained (locked up) or overtly controlled, or to have their passport/identification papers confiscated. Many victims of trafficking have greater freedom of movement and access to mobile phones.

People traffickers are alert to matters raised in court by investigators and prosecutors, and to indicators that alert authorities to potential criminality which are discussed in open-source publications. In response, people trafficking syndicates are changing their modus operandi to avoid detection and, if detected, to make the elements of the offence harder to prove to the standard that satisfies the courts and juries. Law enforcement efforts in Australia are complicated by the fact that the traffickers, victims and evidence of these offences can be located throughout the world and the victims fear retribution by traffickers against themselves and their families. Many victims are reluctant witnesses in legal proceedings.

IRREGULAR MARITIME ARRIVALS

Since 2006, the global refugee population recognised under the United Nations High Commissioner for Refugees (UNHCR) mandate has increased by almost 30 per cent to 11.4 million people. In June 2008, the UNHCR reported that 51 million people were internally displaced, including some 25 million displaced as a result of armed conflict. These internally displaced people are targets for people smugglers worldwide. Displaced persons perceive Australia to be an attractive destination country because of its geographic location and positive economic, political and social environment.

The number of irregular maritime arrivals in Australia decreased dramatically between 2002 and 2007. However, numbers increased from 2008. Since September 2008, there has been a significant increase in arrivals of suspected irregular entry vessels (SIEVs).⁶⁵ In 2008, Australian authorities intercepted seven SIEVs transporting a total of 161 irregular maritime arrivals and 17 crew members. In 2009, this increased dramatically to 60 boat arrivals with 2726 irregular maritime arrivals. By March 2010 there had been four times the number of arrivals seen throughout 2008.

In terms of stated nationality, the majority of irregular maritime arrivals in 2009 were either Afghani or Sri Lankan. Smaller numbers of Iraqi, Indonesian, Iranian, Somali and Burmese nationals have also been recorded. Crew have been predominantly Indonesian, and a small number of Sri Lankan nationals. Reporting indicates a continued threat to Australia from organised people smuggling and, to a lesser extent, independent ventures. Increasing numbers of irregular maritime arrivals are dealing with multiple agents from different supply chains to stage their travel to Australia. This indicates that organisers may be reducing the scope of their operations to focus on moving irregular maritime arrivals between key staging points, rather than guaranteeing their delivery from source countries to Australia.

⁶⁵ A SIEV is a vessel that has been intercepted and is under the control of Australian authorities.



THE RESPONSE



UNDERSTANDING CHANGES IN ORGANISED CRIME AND CRIME MARKETS

Globalisation, changing political, social and economic dynamics and advances in technology continue to create opportunities for exploitation by organised crime. Knowledge of these changes and how they affect the criminal environment helps law enforcement and governments determine appropriate responses and guides operational activity.

The ACC's approach to combating organised crime is determined by the ACC Board. The membership of the ACC Board comprises the Commissioner of the Australian Federal Police (Chair), each state and territory Police Commissioner and the heads of the Australian Security Intelligence Organisation, the Australian Securities and Investments Commission, the Australian Customs and Border Protection Service, the Australian Taxation Office, the Attorney-General's Department and the Chief Executive Officer of the ACC as a non-voting member.

The ACC's *Picture of Criminality in Australia* product suite, which includes the classified *Organised Crime Threat Assessment* (on which this publication is based), informs many Board decisions, including setting priorities and allocating resources.

The *Picture of Criminality in Australia* assessments consider the risks posed by people, groups, markets and other matters affecting the strategic crime environment in Australia and current and emerging trends in criminality and organised crime. Assessments also consider factors that will shape future organised criminal activity. The assessments are crucial decision-making tools for Australian law enforcement. They informed the development of the *Commonwealth Organised Crime Strategic Framework* and are used to guide information collection and set law enforcement priorities and activity through the Organised Crime Response Plan (released on 26 November 2010) and other initiatives.

In these ways, the ACC facilitates a greater national understanding of, and capability to address, key problems such as trends in the production and use of illicit drugs, money laundering and identity crime.

Other markets are monitored to determine changes in the nature and extent of organised criminal involvement. Areas of concern in terms of criminal exploitation include the corporate and financial sectors, high tech crime and intellectual property crime.

Understanding the changing criminal environment is crucial in shaping not only an effective response by Australian law enforcement, but also a collaborative response by agencies outside the law enforcement umbrella which are responsible for regulation and monitoring of key sectors.

The ACC is also collaborating with bodies such as the Australian Institute of Criminology, the National Drug and Alcohol Research Centre and the Australian National Council on Drugs to develop a more holistic picture of the criminal economy, money laundering, various categories of fraud and illicit drug markets. The ACC is likely to benefit from existing or proposed research initiatives by these bodies into several of these areas and can add perspective to the projects through its own datasets and knowledge of the organised crime environment.

Another key component of the ACC's response to organised crime is its High-Risk Funds Methodology. This is an approach to analysing financial data to isolate high risk money movements and identify targets. It involves examining and understanding the criminal economy through economic and analytical modelling of financial, trade and other data drawn from numerous public and private sector sources. Data drawn from overtly recorded money flows is assessed by applying specific algorithms and an agreed threat and risk assessment methodology to identify high-risk funds (that is, those money flows which are most likely to contain illicit funds). Then, entities identified as being associated with the high-risk funds are examined against national law enforcement holdings to identify targets for further development and assessment.

A tailored intervention and prevention response can then be developed in conjunction with the ACC's partner agencies, once again using a risk-based approach weighted to the financial structures and wealth-generating capacity of the criminal organisation.

The benefits of this approach are that it enhances the strategic intelligence picture, more efficiently targets law enforcement efforts to the disruption of criminal enterprises and identifies greater opportunities for confiscating illicit funds.

COLLABORATION

The impact of organised crime on Australian society is significant. It creates economic instability, community fear and risk to personal wellbeing and safety. The use of legitimate activities by organised crime groups disguises criminal activity and makes it more difficult for law enforcement to identify the criminal component.

In dealing with the current and emerging threats from organised crime, law enforcement needs to be flexible, innovative and forward-looking, and will increasingly need to use the skills of highly specialised experts across a broad range of disciplines.





ACC Fusion brand

Collaboration between law enforcement, government and industry is vital in Australia's response to organised crime. High tech crime is a perfect example of the need for broadly based domestic and international collaboration—most IT systems and hardware are owned and operated by the private sector and the risk is sophisticated and multi-dimensional. CERT Australia, AFP and other agencies involved in cyber security are co-located in the Cyber Security Operations Centre to better collaborate and cooperate during cyber security incidents.


Similarly, the Australasian Consumer Fraud Taskforce (ACFT) was formed in March 2005 to increase the level of scam awareness in the community. The ACFT comprises 21 government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams. The ACFT also has a range of community, non-government and private sector organisations as partners.

The purpose of the ACFT is to help government members work together to:

- > enhance the Australian and New Zealand governments' enforcement activity against frauds and scams
- > run an annual coordinated information campaign for consumers—the National Consumer Fraud Week in March (timed to coincide with Global Consumer Fraud Prevention Month)
- > involve the private sector and community groups in the information campaign and encourage them to share information they may have on scams and frauds
- > generate greater interest in research on consumer frauds and scams.

Collaboration will help develop better response strategies that combine the strengths of operational law enforcement activity, regulatory and legislative change and community involvement. Partnerships between law enforcement, industry specialists and governments will offer Australian law enforcement the skills and tools it needs to further improve crime fighting capabilities.

The Minister for Home Affairs and Justice, the Commonwealth Attorney-General and the ACC launched a new Criminal Intelligence Fusion Capability (Fusion) in July 2010, which includes the full range of law enforcement, national security and related Commonwealth agencies. Fusion is maximising the effective use of public and private sector data holdings and facilitating lawful real-time intelligence sharing in relation to serious and organised crime. It is a very practical and cost-effective way of lawfully harnessing a range of data from agencies within government and law enforcement to more effectively direct law enforcement efforts and resources to disrupt the highest-threat criminal targets.



Fusion will increase the ability of the ACC and its partners to integrate data and criminal intelligence to identify high-risk cash flows and patterns of crime as well as the individuals, businesses and corporate structures involved in criminal enterprises domestically and internationally. This capability will also 'fuse' data in near real-time, analyse results and provide actionable intelligence reports to partner agencies.

Fusion exemplifies the advantages of multi-agency responses to organised crime.

INCREASED PUBLIC AND INDUSTRY AWARENESS OF KEY ORGANISED CRIME ISSUES

The Australian public feels the impact of organised crime in numerous ways. There is the money governments invest to fight crime, taxation revenue forgone and the individual and social harm caused by criminal activities, not least of which are the traumatic effects of drug addiction on users and their loved ones. There is the uncertainty that organised crime creates when members of the public interact on the Internet or conduct transactions at ATMs and EFTPOS terminals and the higher credit card rates and insurance premiums that are required to compensate for criminal activity. There are the regulation and reporting mechanisms that apply to pharmacists and suppliers of chemicals to ensure that precursor chemicals are restricted to legitimate uses. There is the distortion to property markets and real estate prices, and the loss of government revenue, caused by mortgage fraud and real estate purchases that facilitate money laundering and other crimes.

Organised crime operates within and alongside legitimate business, gradually corrupting from within. The effect—while hard to quantify or identify until the changes to business ethics more obviously manifest—is cancerous for those legitimate businesses in which organised crime has gained a foothold. All these factors make industry and the public key sources of information about organised crime.

Increased public awareness of the activities of organised crime groups plays a key role in the effective prevention and reduction of such activity. Many frauds are rendered ineffective when the potential victim is able to recognise the attempted crime. Identity crime can be prevented by improving the processes that support identity verification and by educating people in techniques to protect their identities. For example, on 23 November 2009 the Commonwealth Attorney-General launched the booklet *ID Theft – Protecting your Identity*, which provides advice and strategies on how to protect personal and financial information and computer data, appropriate courses of action for victims of identity theft and a list of government resources to help protect personal information.



Card fraud may be reduced by the timely introduction of chip and PIN technology and extortion can be combated by members of the public who report instances of this insidious activity to police. As part of the National Taskforce on Card Skimming, the ACC has been working with the Australian Payments Clearing Association on an awareness-raising initiative. Posters and an education video will be produced and distributed by financial institutions to businesses using EFTPOS terminals, to improve their understanding of card skimming and how to protect these terminals. Awareness and understanding of the risks posed by organised criminal activity will continue to be a vital component of the fight against organised crime in Australia.

The *Cyber Security Strategy* which was launched by the Commonwealth Attorney-General on 23 November 2009 adopts a comprehensive approach to promoting the security and resilience of Australia's information and communications technology systems. The objectives of the Australian Government's cyber security policy are that:


- > all Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online
- > Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers
- > the Australian Government ensures its information and communications technologies are secure and resilient.

On 6 June 2010, the Commonwealth Attorney-General launched a comprehensive publication, *Protecting Yourself Online*, as part of Cyber Security Awareness Week which provides a one-stop-shop for information relevant to Australia's cyber environment.

SPECIALISED LAW ENFORCEMENT STRATEGIES

Organised crime has the capability to resist and adapt to law enforcement efforts. Law enforcement uses special tools including coercive powers, covert intelligence, surveillance and a range of specialised analytical and investigative techniques to overcome this resistance.

Tactical law enforcement responses will, of necessity, continue to be predominantly reactive and directed toward matters affecting single regions and jurisdictions. However, it is recognised world-wide that proactive and specialised law enforcement approaches are crucial to the success of law enforcement efforts in combating organised crime. Once the nature and extent of the organised crime footprint in key markets and sectors is understood, along with the identity and characteristics of persons and networks engaged



in organised crime, the response must include ongoing collaboration between state, territory and Commonwealth law enforcement agencies. The increasing spectre of transnational crime argues for the collaboration to extend to agencies from foreign countries and to world bodies.

THE ACC APPROACH TO COMBATING ORGANISED CRIME

The Australian Crime Commission (ACC) is an independent statutory authority established on 1 January 2003 under the *Australian Crime Commission Act 2002*.

The ACC's primary objective is to support and complement Australian law enforcement efforts to reduce the threat and impact of serious and organised crime. It is a niche, complementary agency which delivers specialist law enforcement capabilities to other agencies in the law enforcement community and broader government. All ACC activities are conducted either with or for one of its many partner agencies across Commonwealth, state and territory governments.

As Australia's national criminal intelligence agency, the ACC provides law enforcement and other Commonwealth, state and territory government agencies with a unique and valuable understanding of serious and organised crime, including its activities, methodologies and emerging areas of influence. To this end, the ACC provides specialist advice on national criminal intelligence priorities and delivers criminal intelligence products and national criminal intelligence information systems.


The ACC also undertakes targeted intelligence operations and investigations into serious and organised criminal activity in partnership with law enforcement agencies under taskforce, joint operation and intelligence-sharing arrangements. Close collaboration with Australian law enforcement and related government agencies is central to the ACC's approach.

The ACC's strategic direction and priorities are established by its Board. A key role for the ACC Board is to approve the use of the ACC's special coercive powers. These coercive powers are an important aspect of its work and of the Australian law enforcement framework, as they allow the ACC to examine witnesses under oath or require the production of documents, or other evidence, in order to collect information that is not obtainable through traditional law enforcement methods.

"All ACC activities are conducted either with or for one of its many partner agencies across Commonwealth, state and territory governments"

ABBREVIATIONS

1,4- BD	1,4- butanediol
ACC	Australian Crime Commission
ADI	authorised deposit-taking institutions
AFF	advance fee fraud
AFP	Australian Federal Police
AML	anti-money laundering
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ATM	automated teller machine
ATO	Australian Taxation Office
ATS	amphetamine-type stimulants
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDPP	Commonwealth Director of Public Prosecutions
Customs and Border Protection	Australian Customs and Border Protection Service
DEA	Drug Enforcement Administration (US)
DDoS	distributed denial of service
DMT	dimethyltryptamine
EFTPOS	electronic funds transfer at point of sale
FARC	Revolutionary Armed Forces of Colombia
FATF	Financial Action Task Force
FIAT	Financial Intelligence Assessment Team
GBL	gamma-butyrolactone
GDP	gross domestic product
GHB	gamma-hydroxybutyrate
GST	goods and services tax
ICT	information and communication technologies
IMA	irregular maritime arrivals
IP	intellectual property
IT	information technology
LSD	lysergic acid diethylamide
LTTE	Liberation Tigers of Tamil Eelam
MBS	Medicare Benefits Schedule
MDMA	3,4-methylenedioxymethamphetamine
NSW	New South Wales
OCGs	organised crime groups



OCRP	Organised Crime Response Plan
OCSF	Organised Crime Strategic Framework
OCTA	Organised Crime Threat Assessment
OECD	Organisation for Economic Cooperation and Development
OMCG	outlaw motorcycle gang
PABX	Public Automatic Branch Exchange
PBS	Pharmaceutical Benefits Scheme
PIEDs	performance and image enhancing drugs
PIN	personal identification number
PKK	Kurdistan Workers' Party
PoCA	Picture of Criminality in Australia
PRC	People's Republic of China
SIEV	suspected irregular entry vessel
SMS	short message service
SMSFs	self-managed superannuation funds
SOCA	Serious Organised Crime Agency (UK)
TBML	trade-based money laundering
UK	United Kingdom
UNHCR	United Nations High Commissioner for Refugees
UNODC	United Nations Office on Drugs and Crime
US	United States
WMD	weapons of mass destruction

