CRIME BULLETIN

CRIME AND MISCONDUCT COMMISSION QUEENSLAND

CRIME BULLETIN SERIES

NUMBER 11, DECEMBER 2009

ISSN: 1442-5815

INSIDE

Information on this series and other CMC publications can be obtained from:

Crime and Misconduct Commission
Level 2, North Tower Green Square
515 St Pauls Terrace
Fortitude Valley Qld 4006
GPO Box 3123, Brisbane Qld 4001

Telephone: (07) 3360 6060
Toll free: 1800 06 1611
Facsimile: (07) 3360 6333
Email: mailbox@cmc.qld.gov.au
Website: www.cmc.qld.gov.au

Money laundering and organised crime in Queensland

A strategic assessment

Summary

The purpose of this assessment is to examine what constitutes money laundering in Queensland and examine different money laundering techniques employed by organised crime groups. It will provide warning signs of particular types of money laundering techniques and discuss law enforcement responses to money laundering, including Queensland proceeds of crime legislation and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth) (AML/CTF Act). This paper will also assess the risk posed by money laundering by organised crime groups.

Understanding money laundering

Why it's important for law enforcement

Money laundering is an important and necessary element of any organised crime network engaged in crimes with a financial reward. Money laundering techniques are also employed by terrorist organisations to access funds required to carry out terrorist activities. Investigating money laundering requires considerable resources and specialised skills, but it is an effective technique for disrupting organised crime groups and limiting and confiscating the proceeds of crime (POC) that they generate.

As identified in previous assessments conducted by the Crime and Misconduct Commission (CMC 2004), individuals engaged in organised crime activities need to legitimise money. However, the definition of money laundering in Queensland is wider reaching than purely legitimising the POC. It includes any transaction involving POC, and is not limited to elaborate techniques to legitimise funds.

Law enforcement agencies (LEAs) are becoming increasingly aware of the value in investigating and identifying money laundering techniques and gathering evidence of money laundering. The key incentives for law enforcement are:

- identification and confiscation of the POC
- quantification of the POC derived by an offender
- identification and prosecution of facilitators and professionals who are assisting organised groups in money laundering activity
- gathering information on new or emerging money laundering techniques that can be used to increase LEA proficiency to ensure similar techniques are identified in later investigations.

There is significant value to be obtained by targeting facilitators of money laundering. An organised group may use professionals such as accountants, financial advisers, brokers and alternative remittance systems (ARS) providers to support more sophisticated money laundering activity. The investigation of and dismantling of

such facilitators will provide significant benefits in disrupting an organised crime group's ability to hide, move and legitimise the POC, and also in impacting on other crime groups who are using the same facilitators. As well, targeting suspected facilitators allow law enforcement to identify, and subsequently investigate, other organised crime groups that use those facilitators.

Abbreviations and acronyms

ABS	Australian Bureau of Statistics
AC&BPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
AFP	Australian Federal Police
AHTCC	Australian High Tech Crime Centre
AIC	Australian Institute of Criminology
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth)
ARS	alternative remittance system
ATM	automatic teller machine
AUSTRAC	Australian Transaction Reports and Analysis Centre
BNI	bearer negotiable instrument
CDPP	Commonwealth Director of Public Prosecutions
CPC Act	*Criminal Proceeds Confiscation Act 2002* (Qld)
CMC	Crime and Misconduct Commission
FATF	Financial Action Task Force
FTR Act	*Financial Transaction Reports Act 1988* (Cwlth)
GDP	gross domestic product
KYC	know your customer
LEA	law enforcement agency
OMCG	outlaw motorcycle gang
PAO	proceeds assessment order
OCDD	ongoing customer due diligence
PJC–ACC	Parliamentary Joint Committee on the Australian Crime Commission
POC	proceeds of crime
PPO	pecuniary penalty order
QCC	Queensland Crime Commission
QPS	Queensland Police Service
SMR	suspicious matter report
SUSTR	report of suspect transactions

Extent of money laundering

The Australian Transaction Reports and Analysis Centre (AUSTRAC) estimates that crime in Australia generates between $2.8 billion and $6.3 billion per annum. However, due to the inherent nature of money laundering and the level of POC that is undetected by LEAs it is difficult to quantify the extent with a high degree of certainty that it occurs in Australia. Whatever the exact figure, money laundering continues to be conducted by organised groups in Queensland to legitimise the POC, and remains a HIGH risk.

Law enforcement investigators in Queensland have traditionally focused on gathering evidence and prosecuting offenders for various offences, but have not always targeted the associated money laundering activity. However, in most crimes with a financial incentive or reward, offenders are also engaged, to varying degrees, in money laundering. There are limited financial investigative resources available to the Queensland Police Service (QPS), particularly in regional areas. This is assessed to have contributed to a gap in intelligence about the types of money laundering techniques used by organised groups. The implementation of civil-based confiscation laws by state and Commonwealth governments in the past few years has resulted in organised groups using more sophisticated money laundering techniques to avoid detection. The greater degree of sophistication may have also contributed to this intelligence gap.

Acknowledgments

In preparing this report, officers from the Strategic Intelligence Unit of the Crime and Misconduct Commission (CMC) consulted with the Queensland Police Service, Queensland casinos, various financial institutions, credit unions and building societies, the Office of Fair Trading, the Australian Crime Commission, the Australian Federal Police, the Australian Institute of Criminology, the Australian High Tech Crime Centre and the Australian Transaction Reports and Analysis Centre (AUSTRAC). We wish to acknowledge the valuable assistance provided by these agencies and their officers.

Lincoln Hansen (Senior Financial Investigator, Strategic Intelligence Unit) was primarily responsible for writing the report and conducting the analyses presented.

The CMC's Strategic Intelligence Unit would also like to acknowledge the assistance provided by other areas of the organisation in completing this report, including the Proceeds of Crime and Organised Crime investigation teams.

The report was prepared for publication by the Communications Unit.

Money laundering techniques

This assessment provides insight into a range of money laundering techniques, the indicators associated with those techniques, and discusses particular case examples. The money laundering techniques employed by organised groups can vary considerably depending on a range of factors, including access to professionals, financial skills and knowledge, nationality and access to contacts in foreign jurisdictions. Money laundering can be as simple as purchasing assets in the name of family members or gambling at casinos. Alternatively, offenders can engage in complicated financial transactions involving international transfers, business structures and cash remittance services. Organised groups are more likely to have access to professional advisers and use more complicated schemes simply because of a greater volume of POC that needs to be legitimised.

A number of laundering techniques are employed by organised groups with varying degrees of complexity. If there is one constant in money laundering techniques, it is the manner in which they can change and adapt to counter law enforcement efforts and regulatory regimes, and to take advantage of technological opportunities. A brief summary of particular techniques is provided from pages 3-5.

Bank accounts

Offenders are more likely to use the bank accounts of associates and family members to distance themselves from their POC. Alternatively, accounts in false names may be used. Accounts in the names of third parties, known as money mules, are also often used by fraud offenders to move the POC to offshore destinations ensuring there is no paper trail linking them to the transaction.

Warning signs of money laundering through bank accounts

Types of account behaviour that are indicative of money laundering include the following:

- An individual or corporate account showing virtually no normal business-related activity or individual expenditure activity. Instead, the account is used as a temporary transit point for funds.
- A bank customer with a large number of accounts that do not appear commensurate with the type of business being conducted or the type of income usually received.
- A large number of transfers between different accounts held by the one customer. Transfers to and from accounts with no apparent explanation may be an attempt to 'layer' funds and create confusion about the original source of the funds.
- Transfers of funds to international jurisdictions associated with dangerous drugs or with weak anti–money laundering regimes.
- Large or numerous cash deposits into an account where the account holder is receiving regular Centrelink or wage income deposits.
- Cash deposit or withdrawal activity that is split into numerous transactions below the $10 000 AUSTRAC reporting threshold in order to avoid detection (known as 'structuring').
- Deposits occurring at a location not normally used by the customer.

Glossary

Bullion
This term describes the precious metals gold or silver in the form of bars or ingots.

Integration
The process of bringing the proceeds of crime back into the legitimate banking or other financial system so as to give the appearance it is from a legitimate source.

Layering funds
The process of conducting various financial transactions in order to mask the true source of proceeds of crime so, as a result, the funds appear that they are from a legitimate source.

Money mule
A person who is recruited, often unknowingly, to receive sums of money into their account and are then required to forward this money back to the organisers of the fraud, and usually involving proceeds of crime.

Pay day loan
A short term loan, usually for a small amount, that is intended to cover the borrower's expenses until their next pay day.

Placement
The initial stage of the money laundering cycle; placement involves conducting a transaction involving the proceeds of crime whereby the physical curreny enters the financial system.

Structuring
The process of breaking down cash deposits into a number of smaller deposits with the intention of avoiding financial transaction reporting requirements by the Commonwealth.

Underground banking
This term describes the process of transferring value between parties outside of the traditional banking systems. There is rarely a movement of physical currency, instead value is transferred often using agents known as alternate money remitters who have a financial, personal or family relationship.

Warning signs of a money mule scheme

For an individual, there are a number of warning signs that indicate a money mule laundering operation, including the following:

- Unsolicited emails offering 'too good to be true' work-from-home opportunities. Individuals should ideally delete such emails or at least verify the legitimacy of a company purporting to offer employment, check their contact details and check where the company is based.
- Job advertisements that simply require the receipt and forwarding of funds. These schemes often require that the funds are transferred out of the mule account immediately and in cash, usually to an overseas destination through a remittance service such as Western Union.
- Jobs that require an individual to open a specific bank account.
- A requirement that individuals provide their own bank account details to receive funds, other than wages, from the 'employer'.
- Poorly written advertisements with grammatical and spelling mistakes.

Alternative remittance systems

Cash remittance businesses known as alternative remittance systems (ARS) are engaged by organised crime networks to send the POC to offshore destinations without detection. These businesses are traditionally used by ethnic groups, but are equally able to be exploited by any organised crime groups. There is a HIGH risk of these businesses being used by organised groups to dispose of significant cash holdings, and a number of examples have been reported in Australia recently.

Cuckoo smurfing and ARS

A money laundering technique relatively new to Australia, named cuckoo smurfing, has been detected in a number of recent instances. The technique is facilitated by ARS that have links to organised crime groups. In a case in 2008, approximately $1.7 million was laundered through a Queensland-based bank account of an innocent third party.

The technique involves a legitimate transaction, independent of the organised crime group, where an individual or business in Australia is expecting to receive funds from an overseas destination. Instead of those funds being received, the organised crime group deposits cash POC to the legitimate recipient's account, and the organised group's POC is made available to them in the overseas location. The technique poses a significant risk to law enforcement, as it allows the POC to be removed from Australia anonymously and avoid confiscation litigation.

Businesses and corporations

Businesses continue to be used by organised crime groups to launder the POC. The business accounts can be manipulated in a number of ways to make the POC appear legitimate. The most common techniques involve the manipulation of either the revenue or the expenditure of the business to make it appear as though the business is more profitable than it is in reality. Cash-based businesses continue to be the most attractive for organised crime groups as they allow for cash deposits to be made into the business accounts without raising suspicion. Examples of these cash-based businesses are convenience stores, restaurants and nightclubs.

Casinos and gambling

There is anecdotal information to suggest that casinos continue to be used by offenders both to expend their POC, and also to legitimise funds through casino chip 'buy ins' and subsequent cashing-out or obtaining casino cheques. Also, there is an indication that offenders are using casino chips as currency in illegal transactions, namely drug trafficking. There is no indication that casinos are being increasingly used for money laundering activities.

Implications for law enforcement

These matters highlight the need for government agencies and LEAs to work with casinos to identify 'high-rollers' who do not have a legitimate source of income. The identification of these individuals and any links they have to organised crime figures will help in locating the source of POC that are later expended through casinos, and assist law enforcement in disrupting the money laundering activities of offenders.

Asset purchases and cash expenditure

Offenders are assessed to be still holding and secreting large cash holdings. This may represent a lack of sophistication on their part, but may also be a result of the increasing reporting and customer risk assessment obligations placed on financial institutions by the AML/CTF Act. Offenders are continuing to convert the POC into assets such as jewellery and bullion, luxury motor vehicles and real estate. More sophisticated offenders are likely to purchase real estate with legitimate funds (including loans) and fund the repayments with the POC. Also, members of organised crime groups are suspected of purchasing real estate in the names of family members and associates with no criminal history in order to avoid confiscation proceedings and to distance themselves from the POC. This provides a degree of difficulty in proving that an offender has effective control of an asset so that it can be targeted for confiscation.

Implications for law enforcement

It is important that LEAs focus on evidence that reveals the level of an offender's cash expenditure, even if there is no longer a particular asset or property that can be seized. The extent of an offender's expenditure (including their cash expenditure) can be used to support drug trafficking and fraud prosecutions by displaying the disparity between an excessive amount of funds expended and assets purchased on one hand, and the relative lack of legitimate income on the other hand. Evidence of cash expenditure can also support POC litigation, and assist the state in obtaining proceeds assessment orders (PAO) and pecuniary penalty orders (PPO). The PAO provides a powerful tool to target the assets of an offender, even in cases when the assets were not purchased with tainted funds.

Identity crime and money laundering

The use of bank accounts with false names remains a money laundering risk, as does the use of accounts featuring the names of associates. The implementation of the AML/CTF Act in 2006 has imposed a number of customer identification and ongoing monitoring obligations that are expected to address this risk and, ultimately, result in a lower number of accounts being opened in false names. Offenders can instead use the identity of associates to conduct illicit transactions.

Stored value cards and debit cards

To date, investigators have only noted a low usage of stored value cards and debit cards, which will be discussed in further detail from page 24. However, some cases have been noted in which such cards have been used to transport the POC out of Australia. It is expected that the use of these cards will grow significantly in the coming years and provide organised crime groups with an avenue to transport funds with relatively LOW risk. Given the global nature of banks and automatic teller machines (ATM), some cards allow funds to be moved offshore without the need to conduct an international electronic transfer (which is reported to AUSTRAC) or the need to conduct bulk cash smuggling. The most effective tool against these cards being used for money laundering will be account holder identification and the monitoring of account activity by debit card account providers pursuant to the AML/CTF Act. The Act imposes obligations on certain cards, depending on the card's threshold value.

Warning signs of money laundering — stored value cards

Debit cards and reloadable stored value cards

In relation to open system cards that can be used to access cash at ATMs, warning signs of money laundering for financial institutions include:

- use of false information or fraudulent documentation to open the account — particular attention should be paid to foreign and even interstate identification documentation
- structured cash deposits underneath the $10 000 reporting threshold
- transactions occurring at unusual locations that are inconsistent with the customer's usual profile
- cash deposits at Australian locations, and withdrawals at an overseas location, on a consistent basis
- requests for multiple cards to access the account
- mailing addresses for replacement or new cards that are inconsistent with the location where the account was opened.

Non-reloadable stored value cards

Warning signs of money laundering for closed system cards that cannot be reloaded or redeemed for cash include the following:

- multiple cards in possession of an individual
- receipts for the purchase of multiple cards
- a history of online access to websites to purchase stored value cards noted from forensic computer analysis.

Implications for law enforcement

A problem for law enforcement is the identification of cards issued by institutions in foreign jurisdictions with weak anti-money laundering regimes. These cards can be obtained using false names with insufficient identification documents and utilised to access funds through Australian ATMs.

Law enforcement strategies

Proceeds of crime

The *Criminal Proceeds Confiscation Act 2002* (Qld) (CPC Act) continues to provide a conviction-based scheme to recover the POC, but also incorporates the civil-based or non-conviction-based scheme. The civil-based scheme provided in the Act has been effectively used to restrain and recover POC and the levels of proceeds of crime litigation have steadily increased in Queensland since the implementation of the Act. To date, in excess of $14 million

has been realised and in excess of $77 million has been restrained through civil-based confiscation legislation. The value of property restrained has increased in 2008–09 compared to the 2007–08 financial year, and this is strongly attributed to the increase in the number of proceeds of crime referrals from the QPS to the Crime and Misconduct Commission (CMC) over this period. It should be noted that, when the property of an offender is restrained, it severely restricts how this property is dealt with by the offender. That is, the restrained property is removed from the criminal environment, precluding it from being used to further other criminal activity.

It is expected that the levels of POC that are restrained and realised will continue to grow in line with an increase in awareness of the civil confiscation scheme among QPS investigators and greater integration of POC recovery into investigation strategies.

A Commonwealth proceeds of crime regime is also well established and used by federal agencies to undertake proceeds of crime investigations and litigation. This regime is set out in the *Proceeds of Crime Act 2002* (Cwlth).

The Anti-Money Laundering and Counter-Terrorism Financing Act

In 2006, the Australian Government enacted the AML/CTF Act. The changes implemented by the AML/CTF Act reflect Australia's response to revised international standards issued by the Financial Action Task Force (FATF) on money laundering and terrorist financing. The Act builds on the financial compliance regime that was previously encompassed by the *Financial Transaction Reports Act 1988* (Cwlth) (FTR Act). The Act continues the regime of reporting certain transactions to AUSTRAC, and has also added reporting requirements relating to the movement of bearer negotiable instruments (BNI) into or out of Australia. The Act has also widened the number of entities that are required to report to AUSTRAC, as it now focuses on the type of service provided, as opposed to defining the entity that is captured by the legislation.

The Act extends to remittance service providers, and requires all remittance service providers to now be registered with AUSTRAC. This obligation should assist in identifying remitters who are non-compliant with the Act, and who are providing an avenue for organised crime groups to launder the POC.

The information collected through the reporting of certain transactions and suspicious matters pursuant to the Act should provide better details of the transaction. The reporting of additional details and information will provide law enforcement with a more thorough understanding of the transactions reported to AUSTRAC, which will in turn provide greater scope to progress and initiate investigations.

The Act also sets out obligations for customer identification and ongoing transaction and customer monitoring which will help law enforcement to identify suspicious transactions and more effectively target money laundering activity.

1: Introduction

This chapter outlines the background to this assessment, describes its purpose and explains the importance of understanding money laundering techniques.

Background

This assessment follows on from two previous strategic assessments compiled in 1999 and 2004. The first crime markets assessment was a joint project (known as Project Krystal) conducted by the then Queensland Crime Commission (QCC) and the Queensland Police Service (QPS) in 1999. The purpose of the 1999 assessment was to explain the nature and extent of organised crime in Queensland across numerous crime markets and to determine current and future risks.

In 2004, the Crime and Misconduct Commission (CMC) compiled *Organised crime markets in Queensland: a strategic assessment* (CMC 2004). This assessment provided an update on the status of markets since the first assessment in 1999 and also identified further markets infiltrated by organised crime networks. This assessment identified that money laundering was perpetrated using offshore accounts, automatic teller machine (ATM) cash withdrawals worldwide, bullion dealers, alternative remittance system dealers, legitimate businesses as a front, and real-estate and luxury asset purchases. The 2004 assessment determined that money laundering posed a HIGH risk and that it was becoming increasingly prevalent.

The 2009 assessment of organised crime markets has been separated into four main portfolios — drugs, property crime, fraud and money laundering. This paper will assess money laundering in Queensland.

Structure of the report

This assessment is presented in five chapters:

- **Chapter 1** sets out the scope and purpose of the assessment, discusses the data collection and risk assessment methodology, and also gives insight into why it is important for law enforcement to understand money laundering techniques.
- **Chapter 2** discusses the inherent difficulty in quantifying money laundering and the present gaps in law enforcement knowledge.
- **Chapter 3** explains a number of money laundering techniques and the warning signs of certain techniques.
- **Chapter 4** summarises two key law enforcement strategies to combat money laundering, namely proceeds of crime legislation, and obligations on reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth) (AML/CTF Act). However, where AML/CTF Act obligations relate to specific money laundering techniques, they are discussed in conjunction with the relevant technique in Chapter 3.
- **Chapter 5** assesses the level of risk to the Queensland community posed by organised crime networks engaged in money laundering.

Scope of the assessment

This assessment examines what constitutes money laundering in Queensland and examines the different money laundering techniques used by organised criminal groups in Queensland.

We also provide insight into the types of financial transactions that Queensland-based offenders carry out, and provide warning signs of particular types of money laundering techniques. The assessment also focuses on law enforcement responses to money laundering, including Queensland proceeds of crime legislation and the AML/CTF Act. In particular, the assessment considers money laundering in Queensland as defined in the *Criminal Proceeds Confiscation Act 2002* (Qld) (CPC Act), and the impact of the CPC Act and the AML/CTF Act. The assessment does not extend to consideration of the specific legislative regimes in other states and territories except for discussion on the impact of the AML/CTF Act on money laundering techniques.

Methodology

Data collection

Information for our assessment was obtained from a variety of sources, such as semi-structured interviews and consultations with several government and law enforcement agencies and private organisations including:

- the Australian Crime Commission (ACC)
- the Australian Customs and Border Protection Service (AC&BPS) in Townsville, Cairns, Brisbane and Canberra
- the Australian Federal Police (AFP) in Canberra, Brisbane and Cairns
- the Australian High Tech Crime Centre (AHTCC)
- the Australian Institute of Criminology (AIC)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the CMC Proceeds of Crime Team
- financial institutions, building societies and credit unions
- the Office of Fair Trading (Queensland)

- casinos in Brisbane, the Gold Coast, Townsville and Cairns
- the QPS.

Other sources include:

- a review of relevant literature including open and closed source material
- relevant law enforcement investigations
- quantitative data from the CMC Proceeds of Crime Team.

Risk assessment

The risk assessment methodology used in this paper is one which was used in both the 1999 and the 2004 CMC crime markets assessments. The consistency in the assessment of risk posed by money laundering allows comparison with previous risk levels. This risk assessment relies on a series of factors to determine the level of risk:

Figure 1: Risk assessment methodology

The risk assessment matrix is essentially a series of formulae to determine level of risk:
Desire × confidence = intent
Resources × knowledge = capability
Intent × capability = likelihood of threat
Likelihood of threat × harm / consequences = RISK

Intent relates to the desire of an individual or group to undertake an activity that also possesses the confidence to succeed.

Capability relates to how realistic it is that the individual or group will be able to undertake the activity, in terms of resources and knowledge.

Threat relates to the likelihood that a person or group will successfully undertake an activity that may cause harm. The likelihood of this success is dependent on their intent and capability.

Harm assesses what physical, psychological, economic and political effects the threat will have should it occur.

Risk is a combination of the threat of an activity occurring and the harmful consequences of that activity.

Definition of money laundering

Money laundering has been defined as the process 'by which illicit source monies are introduced into an economy and used for legitimate purposes' (Walker 1995).

The stages of money laundering are often described as follows:

- Placement — the physical cash proceeds of crime (POC) enter the financial system, through either the normal banking system or an underground/alternative money remitting system.
- Layering — the activity engaged in to create a 'layer' or some distance between the POC and their illicit sources. This can involve complex financial transactions (such as transfers between accounts/individuals/companies) or conversion of the funds from one type to another (for example, by means of bank cheque purchase, casino chips and asset purchases). The key motivation behind layering is to hide the original illicit source of the funds.
- Integration — the entry of POC into the legitimate economy, with a legitimate explanation. The funds appear to have a legitimate source and are able to be expended by the offender without raising suspicion.

However, the definition of money laundering in Queensland is much wider than the commonly understood description outlined above. The actions that constitute the crime of money laundering in Queensland are set out in s. 250(2) to (2B) of the CPC Act. These sections state:

> (2) A person engages in money laundering if the person knowingly or recklessly —
>
> (a) engages, directly or indirectly, in a transaction involving money or other property that is tainted property; or
>
> (b) receives, possesses, disposes of or brings into Queensland money or other property that is tainted property; or
>
> (c) conceals or disguises the source, existence, nature, location, ownership or control of tainted property.
>
> (2A) For subsection (2), a person knowingly does an act mentioned in subsection (2)(a), (b) or (c) in relation to property ***(knowingly engaging in money laundering)*** if the person knows, or ought reasonably to know, that the property is tainted property or is derived from some form of unlawful activity.

(2B) For subsection (2), a person recklessly does an act mentioned in subsection (2)(a), (b) or (c) in relation to property ***(recklessly engaging in money laundering)*** if —

(a) the person is aware there is a substantial risk the property is tainted property or derived from some form of criminal activity; and

(b) having regard to the circumstances known to the person, it is unjustifiable for the person to take the risk.

Accordingly, the act of simply spending the POC — that is, engaging in a transaction — amounts to money laundering under the CPC Act. Our assessment will focus on this wider concept of money laundering and discuss expenditure, as well as schemes to legitimise the POC.

The CPC Act's definition of money laundering incorporates an amendment, effective June 2009, which expands the definition of money laundering to also encompass a person recklessly engaging in activity, as well as knowingly engaging in such activity. It is unknown what impact this amendment will have on the level of money laundering prosecutions within Queensland; however, it will potentially allow professional advisers to be prosecuted in instances when they assist with money laundering schemes even though the state cannot establish that the individual knew the funds were tainted.

Why we need to understand money laundering techniques

In submissions to the 2007 Parliamentary Joint Committee on the Australian Crime Commission (PJC–ACC), the AIC noted that 'the economic driver of serious and organised crime … remains a constant and this will continue to necessitate an understanding of money laundering typologies, both current and prospective' (PJC–ACC 2007).

From a money laundering perspective, the challenge for law enforcement remains the identification of the money trail, and establishing a connection between the individual criminal or group, on one hand, and the POC or the expenditure of those proceeds on the other.

If offenders are prevented from enjoying the spoils of their illegal activities or fined by the courts to the extent that they have earned and expended their POC, the incentive to engage in the illegal activity is severely undermined. Understanding money laundering techniques can help law enforcement to:

- locate the POC
- prove the extent to which POC have been derived or expended by an offender
- identify money laundering facilitators
- understand new or emerging money laundering techniques.

Locating the proceeds of crime

Crime with a financial reward, such as drug trafficking, fraud or theft, has at its core a risk/reward-based decision-making process. Whereas prosecution by law enforcement agencies (LEAs) focuses on increasing the risk involved in criminal activity, the identification and confiscation of POC can have a significant effect on criminal networks as it undermines the incentive or reward for the crime. Understanding money laundering techniques used by organised crime groups is a key element in the identification of the money trail and the end location of the POC.

Quantifying proceeds of crime — expenditure analysis

It is equally important to recognise the value to LEAs of identifying the levels of POC derived and expended by criminal groups, and the associated money laundering techniques. When a high level of expenditure by an offender can be shown, and there is a relatively insignificant level of legitimate income to fund that expenditure, this evidence can be very valuable to support certain prosecutions. Quantifying the POC derived by an offender provides evidence to support the prosecution of offences when a financial element is required to be proven.[1] There is also scope within the CPC Act to use the calculation of an offender's expenditure to obtain a proceeds assessment order (PAO).[2] A PAO allows the state to recover POC from an offender even when there is no criminally derived property in the offender's possession. That is, the PAO is a valuable tool that allows the state to confiscate assets that are legally derived where an offender can be shown to have incurred expenditure but with no legitimate income source. In summary, understanding money laundering techniques will assist law enforcement to gather evidence of the POC derived by an offender which can support criminal prosecutions and proceeds of crime litigation.

1 For example, the offence of trafficking in dangerous drugs set out in s. 5 of the *Drugs Misuse Act 1986* (Qld) refers to 'A person who carries on the business of unlawfully trafficking …'.

2 *Criminal Proceeds Confiscation Act 2002* (Qld) Part 5 — Proceeds Assessment Orders. It is stated in s. 83 that, in an application for a proceeds assessment order, if evidence is given of the amount of a person's expenditure within the past six years the court must treat the amount as proceeds from illegal activity other than to the extent that the expenditure was funded from income not related to an illegal activity.

Identifying money laundering facilitators

By gathering evidence of money laundering schemes and chasing the money trail, investigations are more likely to identify facilitators and professionals involved in assisting organised groups in their money laundering activity. These facilitators can be cash remittance services, accountants, lawyers, other associates or financial service providers. The subsequent prosecution of these individuals will result in a much more effective dismantling of organised crime networks, as it removes their means of dispersing and hiding the POC. The added benefit of dismantling money laundering facilitators is that it will impact not only on the organised crime group being targeted, but also on other groups who are using the services of the same facilitators. This can further assist in the identification of POC as offenders move to other money laundering techniques or facilitators.

Understanding new or emerging money laundering techniques

As money laundering techniques are discovered and documented by LEAs, investigators will gather greater skills in understanding and identifying the various techniques. This understanding will lead to more relevant and useful evidence being seized, an increase in the ability to identify the POC, and greater efficiencies in identifying particular money laundering techniques. It will also assist law enforcement to identify the most useful investigative tools for targeting such techniques. This will result in greater detection and confiscation of the POC and will possibly drive offenders towards cash hoarding and concealment to avoid detection.

2: Extent of money laundering in Queensland

This chapter discusses the cost and extent of money laundering, and the present gaps in law enforcement knowledge of money laundering.

Quantifying money laundering

It is assessed that money laundering is continually expanding in Australia. The increase in reported money laundering indicates that protection of illicit profits is vitally important, irrespective of a group's capability or intent.

Quantifying the extent of money laundering is complicated. A commonly quoted estimate of the extent of money laundering is Michel Camdessus' statement that money laundering is 2 to 5 per cent of global gross domestic product (GDP) (Camdessus 1998). Based on the Australian Bureau of Statistics (ABS) figure for the GDP of Australia in 2007–08,[3] money laundering would be between $22 billion and $56 billion annually. However, according to the Australian Transaction Reports and Analysis Centre (AUSTRAC) in 2007, 'few real advances have been made in the quantification of money laundering at the regional or global levels' (AUSTRAC 2007a). AUSTRAC undertook a significant review of the extent of money laundering in Australia in 2004 and estimated that, within Australia, crime generated between $2.8 billion and $6.3 billion (AUSTRAC 2007a). Whatever the exact level of money laundering in Australia, it is fair to say that a large proportion of organised crime continues to be driven by the derivation and accumulation of the POC. Given this fact, money laundering continues to be an integral part of organised crime activities.

Knowledge of money laundering techniques

In Queensland, there has not been a high level of financial investigative resources applied to the financial element of offences, particularly at the regional level.[4] Feedback from Queensland Police Service (QPS) officers indicate there is minimal access to financial investigative resources in targeting the money trail of offenders. Resources are predominantly applied to the primary offence, such as drug trafficking.

The Proceeds of Crime Team within the Crime and Misconduct Commission (CMC) suspects that at present there is a gap in targeting organised groups in Queensland arising from minimal use of financial investigators.[5] Also, because of the relatively small number of financial investigative resources available to the QPS, in the past these resources have often only been deployed at the closure of operations. Accordingly, there is a knowledge gap regarding the type and sophistication of money laundering techniques.

Law enforcement agencies

An increase in the financial investigative resources available to investigative teams, particularly at the regional level, would benefit the QPS and other law enforcement agencies (LEAs). These resources and expertise would provide agencies with greater capacity to understand and investigate the financial element of crimes. It will assist LEA investigators to target money laundering offences associated with offenders' underlying criminal activity, such as drug trafficking or fraud. The greater availability of financial investigators will also give LEAs an increased ability to gather evidence of an offender's expenditure and the POC derived by that offender. It will also contribute to the identification of POC, which can then be used in confiscation litigation.

With the implementation of civil-based confiscation laws in Queensland, other states and the Commonwealth in the past few years, there have been more effective results in restraining and forfeiting the POC. As a consequence of this more robust approach, organised groups are becoming more sophisticated in legitimising their POC through the use of professional advisers, using existing businesses or establishing new ones.[6] It is assessed that a higher level of sophistication driven by proceeds of crime legislation is also contributing to the gap in detection of money laundering techniques.

It is expected that the wider financial transaction reporting regime resulting from the implementation of the AML/CTF Act will assist LEAs in the detection of the POC. The AML/CTF Act will be discussed further in Chapter 4 on law enforcement strategies.

3 The ABS figure for Australian GDP in 2007–08 is $1132172 million — <www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/DFF44A5EAF864640CA2574F200157646/$File/52040_2007-08.pdf>.

4 Discussions with AFP Brisbane, October 2008.

5 Discussions with CMC Proceeds of Crime Team, November 2008.

6 Discussions with AFP Brisbane, October 2008.

3: Money laundering techniques

This chapter explains a number of money laundering techniques, the warning signs of these techniques and related law enforcement strategies.

Bank accounts

The criminal community appears to have a strong awareness of Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting obligations, and the fact that law enforcement agencies (LEAs) gain access to bank records during investigations. Offenders subject to proceeds of crime litigation rarely appear to use their bank accounts.[7] Accordingly, it appears that the cash proceeds of crime (POC) are being spent on living expenses and other purchases, or being retained as cash holdings.

When bank accounts are used, offenders appear more likely to use accounts of associates or accounts in false names rather than their own accounts. The following case example reflects this.

CASE EXAMPLE 1

The investigation into an offender involved in drug trafficking identified that a number of aliases were used to operate at least 98 bank accounts in a number of different names. The offender used a fake passport and other fraudulent identity documentation. Although the offender did not appear to use the accounts in a sophisticated manner, it highlights the risk of identity fraud being used to hide the POC, and the transfer of funds offshore being undetected.[8]

The warning signs

Types of account behaviour indicative of money laundering include the following:

- An individual or corporate account showing virtually no normal business-related activity or individual expenditure activity. Instead, the account is used as a temporary transit point for funds.
- A bank customer with a large number of accounts that do not appear commensurate with the type of business being conducted or the type of income usually received.
- A large number of transfers between different accounts held by the one customer. Transfers to and from accounts with no apparent explanation may be an attempt to 'layer' funds and create confusion about the original source of the funds.
- Transfers of funds to international jurisdictions associated with dangerous drugs, or with weak anti-money laundering regimes.
- Large or numerous cash deposits where the account holder is receiving regular Centrelink or wage income deposits.
- Cash deposit or withdrawal activity that is split into numerous transactions below the $10 000 AUSTRAC reporting threshold in order to avoid detection (known as 'structuring').
- Deposits occurring at a location not normally used by the customer.

Money mules and money laundering

Offenders are less likely to use their own bank accounts for money laundering. To avoid detection, organised groups engage third parties, known as 'mules', to assist them in moving POC. As discussed in the 2009 Crime and Misconduct Commission (CMC) strategic assessment of organised fraud in Queensland, the use of mules has predominantly been seen in fraud-related crime; however, the technique is equally applicable to moving any other POC. The mule technique is reasonably simple, yet can be a very effective way of transferring funds anonymously.

Elements of a money mule scheme

The elements of a money mule scheme are set out below.

Recruitment of the mule

Offenders often pose as a legitimate company seeking to employ a 'fund manager' or 'financial agent'. They may establish a fake website that appears to be a legitimate business. In some money muling schemes, the money launderers have even purported to be from a known legitimate corporation. The mule's duties as the 'financial agent' are to receive funds and remit them on behalf of the company. Often, these funds have been stolen from the victim's account by the offender who engages the mule. The initial contact between the offender and the mule can occur in a number of ways, including:

- email job offers
- advertising on online recruitment websites
- other advertising.[9]

7 Discussions with CMC Proceeds of Crime Team, November 2008.

8 Discussions with a former QPS investigative accountant, November 2008.

9 Discussions with Australian High Tech Crime Centre, Canberra, July 2008.

Mule bank accounts established

Once the mule has been recruited as an 'employee' of the money launderer, they will either open a new bank account to receive funds, or provide the launderer with the details of their own existing Australian bank account.

Mule receives proceeds of crime and remits overseas

The money launderer transfers funds into the mule's own bank account and the mule subsequently transfers the funds to the final destination. Often the funds are transferred offshore.

The offender is thus able to use the legitimate banking network to facilitate an international transfer anonymously. It is difficult to gauge the extent of this money laundering technique because of the anonymous nature of the technique and the fact that mules may not suspect that they are assisting an organised crime group.

Organised groups in Australia have also used money mules in foreign jurisdictions to implement their money laundering schemes. The following case example illustrates this technique.

CASE EXAMPLE 2

In a recent case in Singapore, an individual (the mule) received an offer by email to be a 'transaction manager' and earn commissions by receiving money and remitting it to Russia and Latvia. The offer purported to be from a bona-fide financial organisation, yet it was actually from an organised crime group that had obtained POC by bank fraud within Australia. The mule received funds from Australia remitted into bank accounts in Singapore through services such as Western Union and Travelex. The mule subsequently forwarded these funds to Russia and Latvia by telegraphic transfers (APG 2008).

This case example shows the complexity that can be involved in money mule arrangements. The money launderers manage to disguise the money trail by involving a number of otherwise unrelated individuals across a number of different jurisdictions.

In some cases the money launderers require the mules to open accounts with specific financial institutions. This technique allows money to be stolen from the victim's account and deposited into the mule account within the same institution. It is believed that offenders are attempting to avoid internal checks by the financial institution, as the initial fraudulent funds transfer is between accounts operated by the same institution. That is, the offender avoids an international funds transfer out of the victim's account, which may be flagged by the institution's computerised systems as a suspicious transaction. The following is a recent example of this scheme.

CASE EXAMPLE 3

In a case noted by an Australian financial institution, the offenders recruited a mule and instructed him to set up bank accounts with particular financial institutions. The mule was under the misapprehension that he was communicating with someone in Russia who might become his bride. He was told by email that the 'sister of the bride' in Australia had money to send to the 'bride' and that he should establish Australian bank accounts with the same financial institutions used by the 'sister'. The offenders then stole funds out of the accounts of Australian victims and transferred these funds into the mule's account. The mule received two deposits from the 'sister'. The first deposit was withdrawn in cash and sent to St Petersburg in Russia by Western Union. The second deposit was able to be seized from the mule's account before it was withdrawn. In this way, the money launderers transferred their POC out of Australia anonymously.[10]

This particular case example also highlights a different mule recruitment technique. In this case, the individual was recruited into unwittingly becoming a money mule through an online dating service. This mode of mule recruitment is particularly difficult for LEAs to detect, as it uses honest people to complete a fraudulent transaction. These individuals most likely have an unblemished history and would be unlikely to raise suspicion with financial institutions. As noted by the Australian Computer Emergency Response Team, the mule does not believe they have been part of a fraud as they have not been required to part with any money (Tung 2008).

Another example of the use of a mule was noted in early 2008 when an offender was jailed in Brisbane for her part in a money laundering scheme. The offender and her de facto partner received approximately $100 000 in POC over a four-month period. Again, the funds were proceeds from banking fraud offences. The offender received commissions for her role in the scheme, and forwarded the funds to third parties overseas. The offenders were detected as the result of complaints by a number of banks whose customers were targeted by the fraud offenders (Flatley 2008).

Warning signs of a money mule scheme

For an individual, there are a number of warning signs that indicate a money mule laundering operation, including the following:

- Unsolicited emails offering 'too good to be true' work-from-home opportunities. Individuals should ideally delete such emails or at least verify the legitimacy of a company purporting to offer employment, check their contact details and check where the company is based.

10 Discussions with a Brisbane financial institution, November 2008.

- Job advertisements that simply require the receipt and forwarding of funds. These schemes often require that the funds are transferred out of the mule account immediately and in cash, usually to an overseas destination through a remittance service such as Western Union.
- Jobs that require an individual to open a specific bank account.
- A requirement that individuals provide their own bank account details to receive corporate funds from the 'employer' for the purposes of carrying out the employer's banking and transaction activities.
- Poorly written advertisements with grammatical and spelling mistakes.

Alternative remittance systems

What is an alternative remittance system?

In 2007, the Australian Crime Commission (ACC) reported that criminals are making increased use of 'underground remittance systems and professional facilitators to structure legitimate business enterprises to camouflage criminal proceeds' (ACC 2007).

Alternative remittance systems (ARSs) are also referred to as 'underground banking' and are often an ethnic-based system founded on a cultural sense of honour and trust. They are informal banking arrangements that allow the transfer of funds both domestically and internationally without using formal financial institutions. They are a legal means of transferring funds internationally and have been used extensively to remit legitimate funds to areas with limited banking facilities, such as countries experiencing civil unrest.

An ARS dealer may have an office in another location or, more likely, will simply deal with other ARS dealers in other locations with which they have a business and sometimes family association. ARSs involve the transfer of the value of currency without a need to physically move the cash or conduct an electronic transfer of funds. The transfer of funds is based on communication between members of the ARS. A basic ARS is set out in Figure 2.

As the diagram shows, the sender is able to send funds to an associate in an overseas location without any electronic transfer of funds or the physical movement of cash. The ARS dealer in Australia now has a debt to the overseas ARS. The ARS dealer overseas may also have clients who wish to send money to Australia, and there will be a flow of cash and instructions opposite to that depicted in the diagram. The debts between the ARS dealers can be settled in a number of ways. For example, the ARS dealers may settle the balance of their debts at the end of each month by telegraphic transfer, or periodically by over-invoicing and under-invoicing. The concept of over- and under-invoicing is explained below.

ARS dealers may also conduct other business activities, which allow an unscrupulous ARS dealer to mask their money remitting business behind the other business activity through under- and over-invoicing. This technique can be best illustrated by an ARS dealer in Australia with an export business. In the following example, the ARS dealer/exporter in Australia sells goods to customers in Hong Kong, and also runs an ARS as a side business. The steps are as follows:

- An Australian crime syndicate engages this exporter/ARS dealer in Australia to send $20 000 to a criminal associate in Hong Kong, and provides $20 000 cash.
- The Australian exporter/ARS dealer sells and ships $100 000 worth of goods to his ARS associate/export customer in Hong Kong, and provides an invoice of $80 000 for the goods (under-invoicing).
- The Hong Kong ARS dealer/importer receives $100 000 worth of goods and only pays the $80 000 invoice to the Australian exporter/ARS dealer.
- The Hong Kong ARS dealer/importer also pays $20 000 to the associate of the Australian crime syndicate.

This example is set out in Figure 3 on page 15.

Figure 2: Alternative remittance system

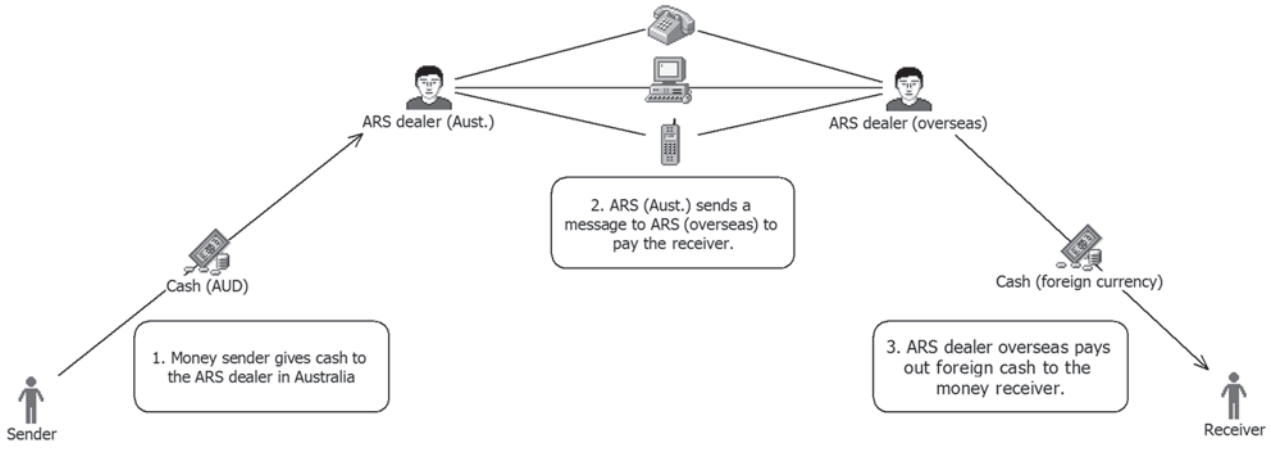
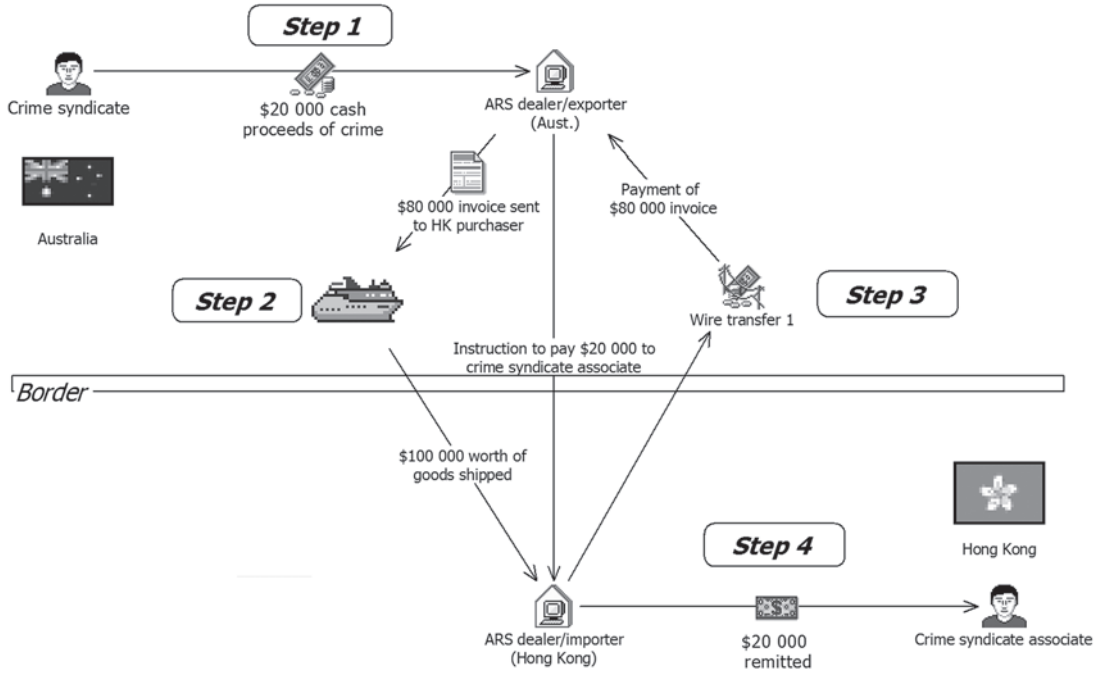


Figure 3: ARS under-invoicing methodology



Organised crime networks and alternative remittance systems

ARSs provide an attractive option for organised crime groups because of the anonymity they can afford and the ability to avoid the regular financial institutions and AUSTRAC reporting obligations. As noted in Figure 2, there was neither an electronic transfer of funds nor any physical movement of cash across the border. Accordingly, ARSs provide offenders with the opportunity to move large amounts of cash with less risk of detection by law enforcement.

The extent to which organised crime groups in Australia are using ARSs and the manner in which they are being used is not fully understood by LEAs. Nevertheless, ARSs have been identified as important money laundering facilitators to organised crime networks in Australia and these services often have offshore associations.

In an investigation reported by AUSTRAC in 2007, a criminal network was involved in importing cocaine from the United States. The network, in an effort to distance itself further from the money trail, recruited third parties at nightclubs to take cash to a remittance dealer, who then wired the funds to the United States (AUSTRAC 2007b).

Law enforcement response

Remittance service providers are bound by obligations under the AML/CTF Act and also some residual obligations under the FTR Act. The arranging of the transfer of money or property is included in the definition of a remittance arrangement under the Act.[11] Accordingly, ARS providers are obliged to report international remittances, significant cash transactions and suspicious matters to AUSTRAC. In addition, the AML/CTF Act also imposes know-your-customer (KYC) obligations on remittance service providers, customer identification obligations, and an obligation to establish an anti–money laundering compliance program for their business.[12] These obligations are discussed in further detail below.

The issue for law enforcement is the extent to which ARS providers supply services to organised crime groups (either knowingly or negligently) and fail to comply with reporting obligations. A drug importation investigation reported by AUSTRAC highlighted the use of ARS dealers to send funds to Vietnam. The ARS dealer was a trusted associate of the offender, and was non-compliant in his reporting obligations under the FTR Act (AUSTRAC 2007b).

In an effort to minimise the risk of money laundering associated with non-compliance by ARS dealers, the AML/CTF Act requires remittance service providers to be registered with AUSTRAC, and also have an AML/CTF program in place and lodge annual compliance reports regarding that program. The Act makes it an offence to provide a remittance service unless registered.[13] It is anticipated that the implementation of this register will help stamp out unscrupulous remittance providers, and also put

11 Section 10, AML/CTF Act.

12 Discussions with AUSTRAC, January 2009.

13 Part 6, AML/CTF Act.

remittance providers on AUSTRAC's radar for monitoring and auditing programs to ensure compliance with the AML/CTF Act.[14]

Recent state legislative reform should also help minimise money laundering by remittance providers. There is now greater scope in Queensland to prosecute remittance providers for money laundering offences. The offence of money laundering was widened in 2009 to encompass 'recklessly engaging in money laundering'.[15] The legislative amendments render it an offence to, amongst other actions, engage in a transaction when the person is aware there is a substantial risk the property is tainted property or derived from some form of criminal activity. As a result of these amendments, remittance providers will be less likely to avoid prosecution by 'turning a blind eye' to the source of their client's funds.

The more stringent regulation of cash remitters may result in money launderers moving towards a more simplistic method of laundering. For example, organised groups may make greater use of false identities to move funds, or engage third parties to move cash on their behalf.[16]

Cuckoo smurfing

A money laundering technique known as 'cuckoo smurfing' has emerged in Australia, with a number of examples reported in recent times. Investigators at the AFP in Queensland have only seen this technique emerging in Australia since 2007, but they have seen examples in Queensland, Western Australia, Victoria and New South Wales. The amount of funds being moved by this technique and the overseas countries involved indicate that it is an emerging money laundering risk that needs to be recognised by LEAs and financial institutions.[17] Cuckoo smurfing is a scheme associated with ARSs that has previously been identified in Europe and the United Kingdom (FATF 2005). The term 'cuckoo smurfing' has its origin in the nesting behaviour of the cuckoo bird. The cuckoo lays its eggs in the nests of other birds, and the eggs are then unwittingly taken care of by these other birds. Similarly, offenders deposit their POC into the accounts of unsuspecting (and unrelated) third parties. The cuckoo smurfing technique involves a legitimate financial transaction occurring through an ARS in one direction, and an illegitimate flow of the POC in the other direction. The scheme basically relies on criminal infiltration, association or coercion of ARS dealers who then 'sell' the legitimate transaction to the organised crime group.

In an investigation conducted by the CMC, a cuckoo smurfing technique was identified when an overseas-based individual wished to send funds to a family member in Australia. The process of cuckoo smurfing in this example involved a number of steps.

Step 1 — Genuine transferor places legitimate funds with ARS dealer

The overseas-based transferor contacted an ARS dealer in his country in order to remit funds to his family member in Australia. This person was a genuine businessman sending legitimate funds. He made cheque deposits into the ARS dealer's account overseas, with instructions as to the accounts where the funds needed to be deposited in Australia. The ARS dealer agreed to perform the transfer and received a commission.

Step 2 — ARS dealer engages organised crime group

The foreign ARS dealer is believed to be involved in the money laundering activities of an organised crime group in Australia. To arrange the legitimate transfer of funds to the Australian recipient, he made contact with the Australian crime group and advised them of the amount of funds and the account details of the recipient. Alternatively, the foreign ARS dealer may have contacted an associated Australian ARS dealer, who in turn made contact with the organised crime group.

Step 3 — Organised crime group effects transfer with multiple deposits

Cash funds, believed to be the proceeds of drug trafficking, were given to a number of individuals to deposit into the account of the recipient. These individuals were the 'smurfs' in the cuckoo smurfing scheme. Investigators have established a link between the deposits and an organised crime group involved in large-scale drug trafficking and importation.

A total of approximately $1.7 million in cash was deposited by the 'smurfs' into the recipient's Australian-based bank account over a six-week period. Although the recipient was based in South-East Queensland, the deposits occurred at a number of different branches around the country. Based on the location and timing of the deposits, they appear to have been effected by three separate cells of individuals, indicating a significant degree of organisation. A total of 61 separate cash deposits, ranging in size from $3500 to $150 000, were made into the recipient's accounts at locations in Sydney and Melbourne. This particular case came to the attention of law enforcement because the financial institution lodged suspicious transaction reports with AUSTRAC.

14 Discussions with AUSTRAC, February 2009.

15 Section 250 (2B) of the CPC Act sets out the provisions relating to recklessly engaging in money laundering.

16 Discussions with AFP Brisbane, October 2008.

17 Ibid.

Step 4 — Organised crime group accesses the proceeds of crime

The organised crime group effectively moved the value of their POC to the overseas location where it was able to be accessed. The ARS dealer in the overseas location can pay the funds as directed by the organised crime group.

The scheme is depicted in Figure 4.

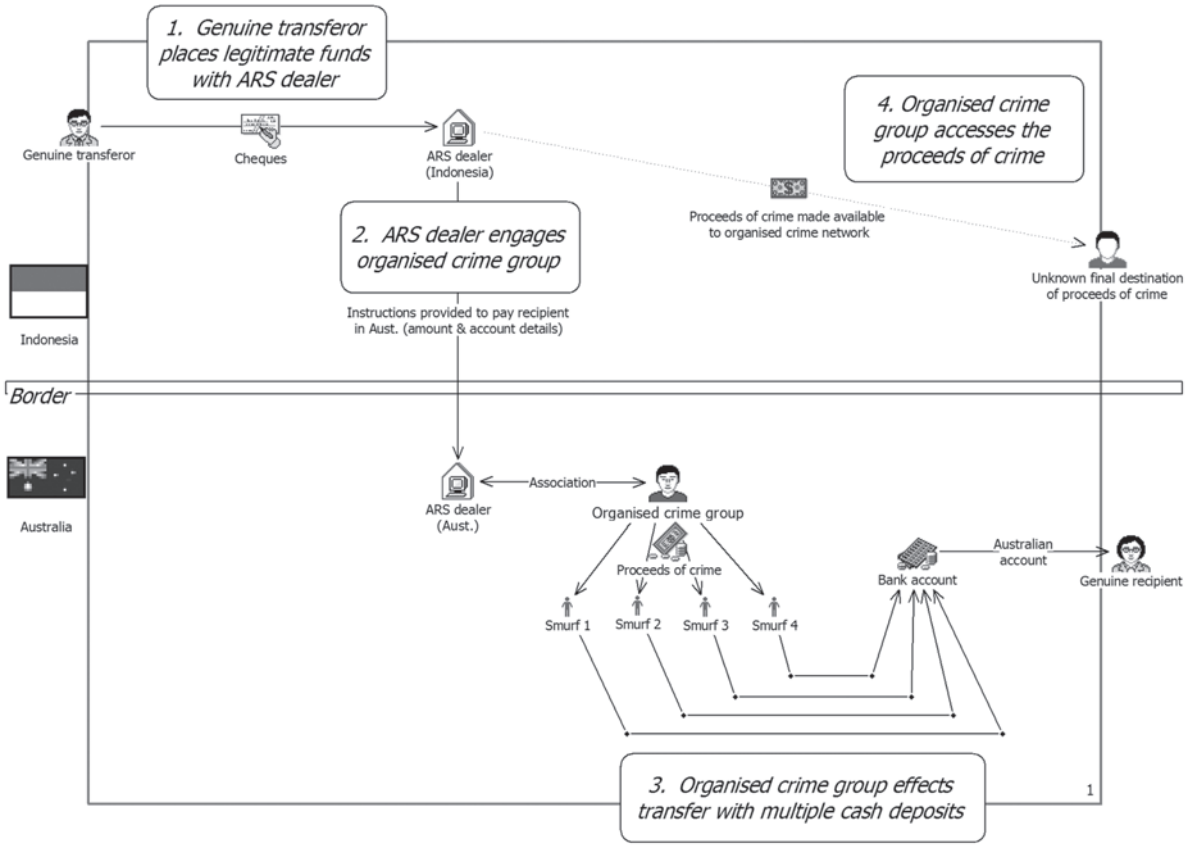
Another investigation in 2008 targeting a drug importation syndicate in Melbourne also noted the use of cuckoo smurfing to launder the proceeds of drug trafficking. It is alleged that the syndicate laundered at least $6.79 million in cash. An individual is alleged to have received cash from the syndicate in amounts up to $1 million, and to have been provided with the names and bank details of accounts where the funds were to be deposited. He subsequently deposited the funds, in amounts ranging from $500 to $25 000, into the accounts of bank customers who were expecting an international money transfer. The POC were then made available to the criminal syndicate overseas (Rout 2008).

Warning signs of a cuckoo smurfing scheme

The most likely point at which cuckoo smurfing can be detected is at the interface with the financial institution. There are a number of indicators of the cuckoo smurfing technique that should be considered by financial institutions. Where unusual activity is noted, financial institutions should attempt to identify depositors, submit a suspicious matter report (SMR) to AUSTRAC and consider retaining CCTV footage that may help law enforcement to identify the depositor. Some cuckoo smurfing indicators are:

- Sudden cash deposits into the account of a genuine person or corporation that are inconsistent with the account transaction history.
- Unusual cash deposits or an unusually large influx of cash deposits that are outside the normal banking practice for a particular account. These deposits may or may not be structured under the $10 000 reporting requirement.
- Cash deposits that are made by someone other than the account holder. As identified by AUSTRAC, cuckoo smurfing exploits the lack of identification of persons (the smurfs) who are depositing funds into the accounts of third parties (the genuine recipient) (AUSTRAC 2008).
- Deposits conducted at branches or locations that differ from the normal banking activity. The smurfs are not necessarily based in the same location as the account holder, and sudden transactions in unusual locations can be indicative of cuckoo smurfing.

Figure 4: Cuckoo smurfing



Businesses and corporations

Offenders continue to use businesses and corporate structures to distance themselves from asset ownership, as well as to provide a vehicle to legitimise POC. The extent of sophistication noted in investigations can vary widely. In some cases, existing legitimate businesses have been purchased by offenders. In others, the business names and corporations exist only on paper to facilitate money laundering activities. Many outlaw motorcycle gang (OMCG) members are noted as having registered companies.[18]

In a recent case, an offender generated income through the sale of heroin. The offender engaged professional advice to set up a company and family trust through an accountant. He also set up a business and a website that purported to be involved in sweeping premises for electronic devices, debt collection and money lending. When he was raided by police, there were no real business records. The business in this case appeared to be simply a 'front' to explain the source of funds generated through the trafficking of illegal drugs.[19]

QPS investigators suspect that there are businesses used by organised crime groups in South-East Queensland to receive POC. Known offenders in South-East Queensland have purchased businesses, expensive real estate and motor vehicles, yet their identified sources of income are only small businesses that appear unlikely to support such purchases.[20]

How businesses are used to launder money

The simple answer to this question is that offenders make the POC look like they are actually the proceeds, or income, of the business. There are a number of ways to do this, with varying levels of sophistication. Simply put, a business earns revenue from its customers and incurs expenditure through payments to its suppliers and employees. In almost all examples, the laundering technique focuses on one or both of the revenue and expenditure elements of the business. Revenue can be made to look larger than it actually is by injecting POC into the business. Alternatively, business expenses can be made to look smaller than they actually are by being paid with the POC instead of through the business accounts.

Manipulating the revenue of the business

Laundering POC through revenue manipulation of a business involves depositing the POC into the business accounts and claiming them as part of the business's legitimate revenue. The scheme is depicted in Figure 5.

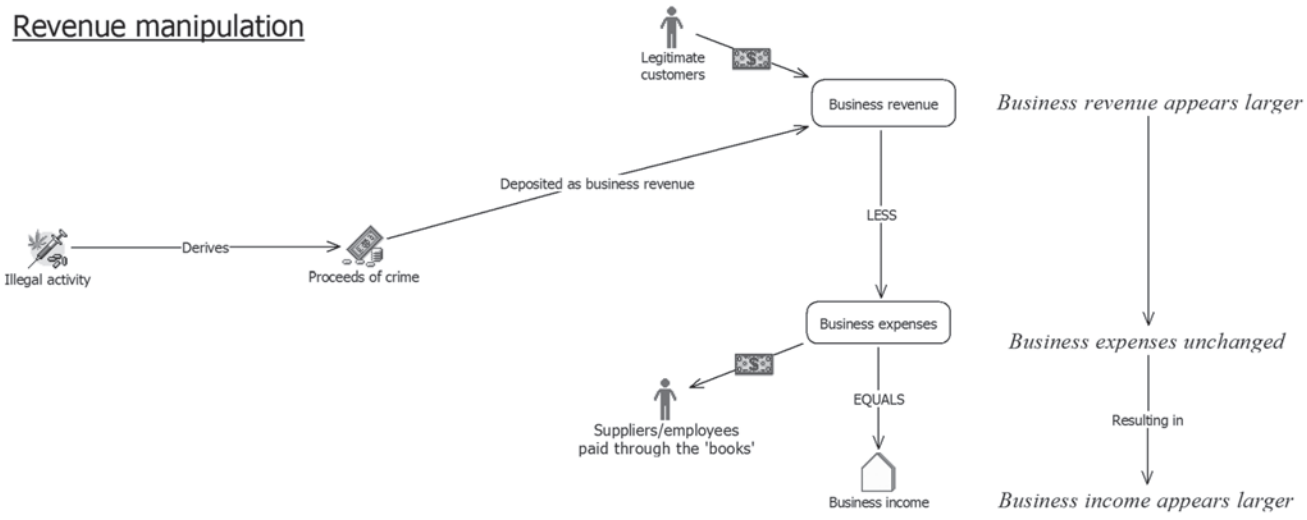
The POC are added to the legitimate business revenue and deposited into the business bank accounts. The revenue and overall business income appear larger than the actual figures.

18 Discussions with QPS Task Force Hydra, October 2008.

19 Discussions with CMC Proceeds of Crime Team, November 2008.

20 Discussions with QPS Metropolitan South Region, October 2008.

Figure 5: Money laundering through business revenue manipulation



In many crime markets, the POC are traditionally in cash. Therefore, offenders are most likely to use a business that has legitimate cash income to engage in this money laundering scheme. The AFP noted that Israeli organised crime groups are likely to own cash-generating businesses, such as convenience stores and restaurants, and feed the POC into these businesses to make it appear that they are generating a higher level of legitimate income.[21] Financial investigations are therefore complicated by the difficulty of quantifying the level of legitimate cash income versus the POC filtered into the business. Many OMCG members own businesses such as security firms, motor vehicle dealerships, panel beaters, auto repair workshops, tattoo shops and concreting businesses.[22]

CASE EXAMPLE 4

In a recent investigation, an offender associated with OMCG members owned an automotive upholstery business. There were many sales invoices with only a minimal number of details recorded. Investigators suspected that significant illegitimate cash was being laundered and pumped into the revenue of the business. This suspicion was reinforced when the business was sold, as the new owner noticed a large dip in the cash sales.[23]

Manipulating the expenditure of the business

Laundering POC through expense manipulation of a business involves paying some of the business expenses in cash with the POC. This reduces the need to withdraw funds from the business accounts. The scheme is depicted in Figure 6.

As fewer funds need to be withdrawn from the business bank accounts, business expenses appear smaller and overall business income appears larger than the actual business income.

This scheme is more sophisticated than revenue manipulation as it requires the cash POC to be given to third parties and records of payment to be kept outside the legitimate business records. However, it is a versatile scheme in that it can be employed in non-cash businesses quite effectively, without raising the suspicion of or detection by law enforcement. As no 'dirty cash' is being put into the business accounts, they appear quite normal. The following case example discusses this money laundering technique.

CASE EXAMPLE 5

A financial investigation completed in 2008 involved persons engaged in drug trafficking in South-East Queensland. One of the individuals also ran a successful legitimate business. Financial analysis of the banking patterns of this business did not show any particular irregularities. The business earned legitimate income that was usually received into the business accounts by way of direct deposit. It had minimal cash revenue. Business expenses were also noted from cheque withdrawals from the business bank accounts. However, a comparison of the business's computerised accounting records and banking records revealed a number of anomalies. There were a number of expenses noted in the accounting records that were not matched by withdrawals from the business bank accounts. It appears that the offender used cash earned from illegal activity to pay a number of the business expenses directly. These expenses were predominantly wages, with some smaller invoice and petty cash expenses.[24]

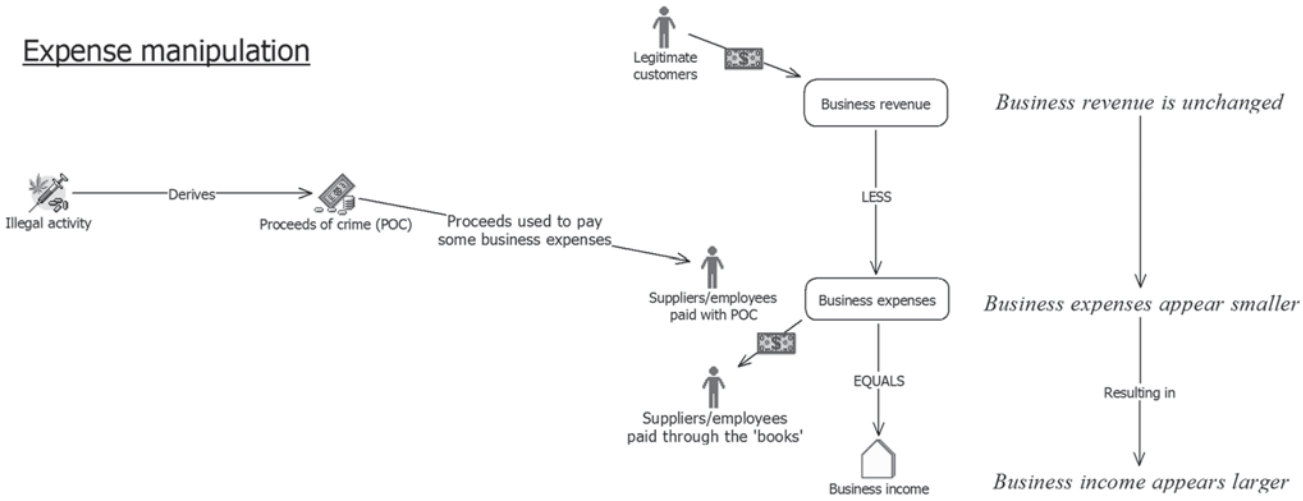
21 Discussions with AFP Brisbane, October 2008.

22 Discussions with QPS Task Force Hydra, October 2008.

23 Discussions with a former QPS investigative accountant, November 2008.

24 Discussions with CMC Organised Crime Team, November 2008.

Figure 6: Money laundering through manipulation of business expenditure



Money can be laundered through businesses anonymously by engaging third parties to be the business owners on paper, and channelling the POC into business establishment costs, as well as the business expenses. Case example 6 reflects this practice.

CASE EXAMPLE 6

In a QPS investigation, a known drug trafficker entered into a business relationship with a third person. The third person arranged for the establishment of a number of businesses, including leasing premises, and the offender provided cash POC to fund the business set-up and the payment of contractors. This allowed the offender to place POC into the business asset while remaining anonymous. The offender continued to launder money through these businesses by paying employees with cash POC. The businesses in this case did not include the full wage expenses in tax returns, and on paper the businesses simply appeared more profitable. The offender also had an interest in another business where, again, the bulk of the employees were paid in cash POC in order to launder the funds and have them appear as legitimate business income.[25]

Laundering the POC through either revenue or expense manipulation of businesses provides offenders with an additional benefit in that they are able to sell the businesses at an inflated price, given the artificially inflated trading profits. It also affects other businesses that are providing comparable goods and services legitimately. As the money laundering enterprise is bolstered by the POC, the offender is able to provide the legitimate services of the business at a cheaper price. Accordingly, the profitability and livelihood of legitimate businesses can be damaged by the involvement of organised crime elements in particular business sectors.

Loans to third parties and associates

Loans to third parties, and particularly to criminal associates, can be an effective way of laundering POC and avoiding confiscation by law enforcement. If the cash funds cannot be physically located, and no other physical evidence of the loan exists, the offender will be able to avoid confiscation action to the extent that he or she has been able to offload those cash funds to third parties.

An offender in a CMC proceeds of crime matter lent suspected POC to a criminal associate, secured against $300 000 worth of diamonds. Offenders have an incentive to either keep no records or keep coded records when laundering POC through loans to criminal associates. This example also highlighted another money laundering technique, namely the conversion of POC into valuable items such as jewellery and precious stones.

Another case investigated by the CMC highlighted how an offender generated proceeds from illegal activity, and then conducted a business to lend these funds through arm's-length transactions. In this case, the loans were well documented. Again, this case illustrated jewellery being used as security for the loans.

Recent changes to Queensland legislation have imposed an annual interest rate cap of 48 per cent on Queensland credit contracts from 31 July 2008.[26] The imposition of this cap has put more than 200 loan centres out of business and driven the 'pay day loan'[27] business underground — into the hands of OMCGs, according to a pawnbroker industry representative (Lutton 2008). Similar interest rate cap legislation is already in place in New South Wales and Victoria. Whether a shift in lending to organised crime groups will occur in Queensland remains to be seen at this stage. The chair of the Australian Financial Counsellors and Credit Reform Association said that 'claims by pay day lenders that a 48 per cent interest cap makes their business unviable had not been borne out in the states such as Victoria and New South Wales' (Tipper 2007).

Casinos and gambling

The exact level of money laundering in casinos is not well known in Queensland. There have been some cases noted where offenders have attempted to legitimise funds using casinos. For example, there is anecdotal information that casinos are being used to launder money by 'buying in' with cash derived from illegal activity, obtaining gaming chips, and subsequently cashing out. The offenders then have the receipts to 'prove' that the money is legitimate.

25 Discussions with QPS Drug Squad, November 2008.

26 Section 3 of the Consumer Credit (Queensland) Special Provisions Regulation 2008, and s. 14 of the *Consumer Credit (Queensland) Act 1994*.

27 A 'pay day loan' is a short-term cash advance that is made to an individual, usually in order to cover living expenses that need to be paid before the individual's next payday. Usually, the interest rate charge is quite high, and the individual is expected to repay the loan with their next pay cheque.

In terms of money laundering, the larger issue concerning casinos is the level of tainted funds expended by offenders. As noted previously, the definition of money laundering includes a transaction involving, and a disposal of, money that is tainted property. In many proceeds of crime cases in Queensland, the offenders have a history of casino and other gambling activity.[28] Recent media reports highlighted a large number of individuals in receipt of Australian Government welfare payments expending large sums through casinos nationwide. It is reported that 329 pensioners and Newstart Allowance recipients, who receive benefits of less than $300 per week, managed to 'buy in' with $45 million of gaming chips across Queensland's four casinos over a 16-month period (Viellaris 2008). It is unknown whether the welfare recipients are involved in money laundering on behalf of organised crime groups. At any rate, the matter highlights the need to identify casino patrons, and the benefits that can be obtained through sharing of information between casinos, LEAs and other government agencies such as Centrelink.

Identification of casino patrons

A number of factors contribute to the difficulty of identifying money laundering in casinos. One of the key problems limiting the assessment of money laundering is that of identifying casino patrons. Casinos are required to report cash transactions of $10 000 or more and suspicious matters to AUSTRAC, pursuant to the AML/CTF Act. In these instances, the identity of the depositor is obtained. Identifying gambling patrons is complicated by factors such as patrons holding false documents in alias names, and even being in possession of identity documents of third parties.[29]

Exclusion of individuals under the *Casino Control Act 1982* (Qld)

The potential exists to reduce the amount of tainted funds expended through Queensland casinos by excluding relevant individuals pursuant to the *Casino Control Act 1982* (Qld). Casinos have the power to exclude individuals pursuant to s. 92 of the Act. Historically, because of the scope of the power granted by the Act, Queensland casinos tend to exclude persons only if an offence has been committed while at the casino, and would rarely venue-exclude a person for external criminal activity without strong information in support. A power to exclude in these cases is granted to the Commissioner of Police under s. 94 of the Act; according to casino industry representatives, however, this power does not appear to be commonly used in Queensland. Nevertheless, over the past 18 months, QPS investigators from Townsville have commenced proceedings against individuals for exclusion offences pursuant to the *Casino Control Act 1982* (Qld).

Discussions with members of the casino industry indicate that the power granted to the Commissioner of Police could be used to exclude individuals who have a history of criminal activity outside casinos, and who may be expending tainted funds in Queensland casinos. The QPS Casino Squad indicated that the New South Wales Police Casino Crime Squad work in conjunction with casino investigators to identify persons of interest who are possibly expending POC at casinos.

Legitimising funds through casinos

Recently AUSTRAC information suggested that alleged money launderers were using Australian casinos to launder their POC by purchasing and cashing out chips with no gambling activity, and putting cash into slot machines and claiming credits as jackpot wins (AUSTRAC 2007c). It is possible for an offender to 'buy in' with cash anonymously (either on their own behalf, or by engaging associates) below the AUSTRAC reporting threshold of $10 000. If this is done on a number of occasions, they can accumulate a substantial value of gaming chips. Discussions held with the QPS suggest that — as well as gambling in their own right — crime groups may also engage mules to gamble in casinos.[30]

The following case illustrates an example of significant chip cash-outs coupled with minimal casino gaming play.

CASE EXAMPLE 7

AUSTRAC recorded an instance in 2007 where an individual involved in illegal drug importation was involved in a high degree of casino activity. The individual had a total value of chip cash-outs of $890 000, yet had minimal recorded casino gaming play. The assumption was that the proceeds from illegal drug trafficking were used to purchase gaming chips, cash out and claim the funds as casino winnings (AUSTRAC 2007c).

Other gambling issues

In South-East Queensland, casino chips appear to be used outside the casino as a form of currency, especially within the Asian community. Casino industry representatives noted that, during 2008, the number of gaming chips missing from the casinos had been increasing. It is unknown to what extent these gaming chips being removed from the casinos are sourced from tainted funds; however, it is believed that they are being used by individuals involved in drug trafficking.

28 Discussions with CMC Proceeds of Crime Team, January 2009.

29 Discussions with casino industry representatives, November 2008.

30 Discussions with QPS Metropolitan South Region, October 2008.

There is some suspicion that offenders purchase tickets from legitimate winners at TAB outlets in hotels and clubs.[31] Alternatively, the offender may request the return of the winning tickets from the TAB officer. The offender then claims that the gambling win is the legitimate source of their cash. It is not suspected that this method is employed by larger organised crime groups. The following case illustrates a similar occurrence in NSW, where individuals purchased legitimate winning jackpot cheques.

CASE EXAMPLE 8

A group of overseas nationals purchased winning jackpot cheques from legitimate winning individuals in various clubs in New South Wales. About $1.7 million in winning cheques was deposited into accounts and withdrawn in cash, providing a legitimate source of the cash holdings and subsequent cash expenditure by the overseas nationals (AUSTRAC 2007c). In this case, although the original POC may have been generated outside Australia, Australian individuals (the actual winners) have played a part in a money laundering operation.

Asset purchases and cash expenditure

Why is evidence of cash expenditure important?

Financial investigators can use evidence of cash expenditure of an offender to:

1. Show the disparity between asset purchases and cash expenditure on one hand and the level of legitimate income on the other hand. If an offender incurs substantial expenditure such as asset purchases or lifestyle expenses with non-existent or minimal legitimate income to justify that expenditure, this can be valuable circumstantial evidence to support charges such as drug trafficking or fraud.
2. Support an application for a proceeds assessment order (PAO) under the CPC Act. As discussed earlier, a PAO can be obtained in certain circumstances to deprive an offender of cash and assets regardless of whether or not they have been derived directly from the POC. There is also scope under the CPC Act to obtain a pecuniary penalty order (PPO) for the amount of the benefits derived by an offender through the commission of a confiscation offence.[32] Quantifying the value of asset purchases and funds expended will assist in calculating the benefit derived.

31 Discussions with CMC Proceeds of Crime Team, November 2008.

32 A 'confiscation offence' is defined in s. 99 of the CPC Act.

Cash movement and expenditure

Within the drug market in Queensland, cash is very much the trading medium, although there is some evidence of jewellery and gold, and even casino gaming chips, being used.

Cash still appears to be held by many offenders within Queensland. That is, they have been unable or unwilling to launder the POC further. This may be the result of a lack of sophistication in money laundering techniques, or a reflection of offenders' preference for simply purchasing goods and services with cash in a manner that avoids detection. The Proceeds of Crime Team of the CMC made three cash seizures of approximately $700 000 each during 2008. It has also been noted that offenders often generate large amounts of cash that they have difficulty disposing of or legitimising, resulting in large sums of cash being located during the execution of search warrants.[33]

It is suspected that quite a high level of cash is still being moved offshore by criminal networks. In a matter reported to AUSTRAC, the owners of a brothel understated the income from the brothel and laundered the undeclared component of the income through cash smuggled out of Australia, as well as bullion purchases and loans to associates (AUSTRAC 2007c).

In a number of investigations in Queensland, it has been found that offenders are putting cash into home renovations and paying subcontractors in cash. In 2008, an individual involved in drug trafficking is believed to have spent about $1 million building a house while receiving Centrelink benefits. In 2007, an investigation by the CMC Organised Crime Team also identified an offender who expended considerable cash on home renovations.

Investigations in Queensland have also identified many instances of offenders paying their legal representatives in cash. This cash may be paid by an associate or family member, and is often believed to be the POC derived by the offender.[34]

Real estate

There is evidence that offenders convert POC into real estate. The level of sophistication employed can vary. In one instance, an offender used $600 000 in cash in purchasing a house worth $1.3 million. The offender sought to explain the cash by obtaining a statutory declaration from a family member stating that the money was a gift. Individuals have also been noted in a number of instances to purchase

33 Discussions with QPS Metropolitan North Region (Redcliffe), October 2008.

34 Discussions with QPS Drug Squad, November 2008, and CMC investigators, November 2008.

bank cheques with cash for amounts underneath the $10 000 reporting threshold. Multiple cheques are then provided to a solicitor to fund the purchase of real estate.[35] More sophisticated offenders have proven to be less blatant in their purchases. They often take out mortgages, and use companies or even third parties as the legal owners of the real estate.

In South Australia, OMCG members were noted to amass a large real-estate portfolio. Members borrowed heavily to fund the purchases, and often rented the premises to associates. It is suspected that proceeds from drug trafficking were used to finance the house loans.[36]

Intelligence gathered by the QPS indicates that Russian nationals are purchasing expensive real estate on the Gold Coast. Some of these people have links to organised crime groups in Australia. Often the real estate is not encumbered by a mortgage. It is likely that the POC have been derived outside Australia, and the real-estate purchases represent the integration step of the money laundering process.

It is believed that offenders, particularly within the Asian community in South-East Queensland, are likely to purchase real estate in the names of associates or family members, who are also responsible for the debt incurred to support such purchases. Instances have been noted where false employment and income particulars and documentation have been provided in support of the housing loan applications. This practice highlights the need for a high level of vigilance on behalf of lending institutions to ensure that the 'purchaser' has a bona-fide source of legitimate income to support the level of debt incurred.

The QPS has noted instances of real estate and businesses being purchased by offenders who falsify legal documents with a reduced sale price. The offender is able to extract the POC at a later date by selling the asset at market value. This type of money laundering technique is able to be detected using covert sources and financial analysis to detect the existence of unusual cash wealth or expenditure.

Bullion and jewellery

Within Proceeds of Crime investigations at the CMC, investigators have noted repeated instances of offenders selling gold to the Australian Mint. The original source of the gold is believed to be melted-down jewellery that has been obtained illegally. The offenders subsequently explain their wealth through the invoices and receipts from the Mint evidencing the sale of gold.

QPS officers have also noted an increase in the amount of gold jewellery that is owned by OMCG members. It is uncertain whether members are acquiring this jewellery through theft, drug transactions or other means. There is also intelligence linking OMCG members to jewellers in Queensland which are used to dispose of gold.[37]

In a matter reported by AUSTRAC in 2008, an offender used cash to purchase silver bullion. About $180 000 worth of silver was purchased, using structured amounts of less than $10 000 to avoid AUSTRAC reporting obligations. The offender also used third parties to undertake bullion purchases on his behalf (AUSTRAC 2008).

A more sophisticated scheme involving jewellery has been used by Asian networks in South-East Queensland. Asian organised crime groups are believed to be sending POC in the form of gold and jewellery to Vietnam, where it is re-identified and sold. The proceeds from this jewellery are then converted into other assets or sold and the offender then brings the proceeds back into Australia with paperwork to suggest it is the legitimate sale proceeds of a foreign asset.

Overall, there does not appear to be an increase in the use of gold or jewellery to hide or move the POC. It is a constant means of laundering money that appears relatively unchanged.[38]

Other assets

There is a tendency for younger and unsophisticated offenders, especially within the illegal drug market, to use the POC to purchase expensive lifestyle items such as motor vehicles, boats, jet-skis and motorcycles. Members of OMCGs tend to own a motorcycle worth up to $60 000 and motor vehicles worth between $50 000 and $100 000. Although they frequently live in expensive houses, these are often rental premises.[39] The challenge for law enforcement is identifying high-value asset purchases including those registered in the names of offenders and their associates.

Identity crime and money laundering

As discussed in the CMC assessment *Organised fraud in Queensland* (CMC 2009), identity fraud remains a growing problem in Queensland and in Australia generally. Both identity theft and the use of false identities have been used to perpetrate a large number of fraudulent offences. However, it is equally important to recognise the risk that identity crime poses in relation to money laundering. The creation of

35 Discussions with AFP Brisbane, October 2008.

36 Discussions with ACC Canberra, July 2008.

37 Discussions with QPS Task Force Hydra, October 2008.

38 Discussions with AFP Brisbane, October 2008.

39 Discussions with QPS Task Force Hydra, October 2008.

a false identity allows an offender to operate accounts, hold assets, transfer funds offshore, and generally avoid detection when dealing with the POC. There is a particular risk involved in a false identity being used to transfer funds out of Australia, as the offender is able to remove the POC from Australia anonymously. The funds become a resource that can then be used for lifestyle expenditure overseas or to fund further illegal activity.

According to the AFP, to be effective in defeating the AML/CTF Act reporting obligations[40] an offender ideally needs a separate identity. This identity may be a false identity, a stolen identity or an innocent third person.[41] As discussed in earlier examples, offenders often use other identities in their money laundering techniques, such as:

- innocent third-party bank accounts being used — cuckoo smurfing
- using family member bank accounts for cash deposits
- holding assets in the names of associates
- using associates to receive funds from overseas
- transferring funds into the accounts of money mules.

It is expected that the increased know-your-customer (KYC) and ongoing customer due diligence (OCDD) obligations imposed on reporting entities by the AML/CTF Act will contribute to a decrease in the level of identity crime perpetrated on financial institutions and hence in the level of money laundering risk associated with identity crime. Whether these are effective in the battle against identity crime remains to be seen. These AML/CTF Act obligations are discussed in further detail below.

Prepaid stored value cards and debit cards

Prepaid stored value cards are cards preloaded with a fixed amount of value or currency on a magnetic strip or a computer chip embedded in the card. The value can be transferred to merchants in a manner similar to spending physical currency. Closed system cards are typically limited to the purchase of goods or services from the merchant issuing the card. They are typically anonymous and non-reloadable (Choo 2008). Examples of these cards are Bunnings and Myer gift cards. Open system cards are typically connected to global debit and automatic teller machine (ATM) networks, and they are typically reloadable and not anonymous but usually embossed with the customer's name. An example of this card is the VISA cash passport card (Choo 2008).

Research in the United States estimates that prepaid debit card spending will increase from US$12.8 billion in 2004 to US$150 billion by 2009. Given this massive potential growth, concern has been expressed in the United States that the increasing number of transactions will make illicit transactions more difficult to detect, thereby providing drug traffickers and other offenders with more service options for moving their POC (NDIC 2006).

The extent to which stored value cards are used by offenders to perpetrate money laundering is unknown in Australia at this stage. However, given the likely increase in these types of products in the future, combined with the adaptability of offenders to new money laundering techniques, there is some risk in stored value cards being used for money laundering. Debit cards allow funds to be easily moved and accessed internationally, as can be seen in the following case example.

CASE EXAMPLE 9

Funds from a fraud in another country were transferred to a Vanuatu bank account. The accounts in Vanuatu were opened using a local lawyer and the POC were deposited as 'business sales'. The offender advised the bank that the funds were deposited to pay business-related expenditure. The funds were actually withdrawn in small amounts in several European countries, using an international debit card (APG 2008).

Risks associated with open system cards

Open system cards offer offenders an attractive option for moving funds offshore without detection and with less risk than bulk cash smuggling. There is no requirement in the AML/CTF Act for an individual to declare that they are carrying stored value or debit cards. As these cards can often be used in a foreign jurisdiction to withdraw cash from an ATM, they allow the transport of funds out of Australia without risk of detection.

It is arguable that reporting obligations, similar to those imposed by the AML/CTF Act regarding physical currency and bearer negotiable instruments (BNI), should be implemented to cover a person physically taking, mailing or shipping a stored value card out of Australia. However, it would be difficult to police such a legislative reform, because of the ease of concealment of cards. Another money laundering risk associated with open system cards was noted by the Serious Organised Crime Agency in the United Kingdom. Offenders could move funds offshore through debit card accounts without the need to ever physically send the card. Offenders with access to the appropriate experts in card technology can simply load value onto a debit card

40 For example, Threshold Transaction Report of cash transactions of $10 000 or more — s. 43 AML/CTF Act, International Funds Transfer Instruction Report — s. 46 AML/CTF Act, and Suspicious Matter Reports — s. 41 AML/CTF Act.

41 Discussions with AFP Brisbane, October 2008.

in Australia, and send the personal identification number (PIN) and the card track data to an overseas associate by email or other means. This information can then be cloned onto blank cards in the foreign jurisdiction for subsequent withdrawal of the POC through ATMs (SOCA 2008).

The following case examples show the relative ease with which funds can be moved internationally by criminal groups using open system cards.

CASE EXAMPLE 10

An individual in Australia was part of a syndicate involved in cocaine importation from South America. This person operated an account with access to stored value cards and obtained multiple cards to allow cash to be obtained by him and his associates in multiple locations around the world. It was noted that this person deposited approximately $400 000 cash, in structured amounts underneath the $10 000 reporting threshold, into accounts in both his own name and that of an associate. The funds were subsequently withdrawn at various ATMs in South America (AUSTRAC 2007c).

CASE EXAMPLE 11

A group of individuals purchased United States dollar stored value cards in Australia with multiple cash deposits between $8000 and $9700. These accounts could then be used in the United States to withdraw the funds in cash without an international funds transfer. The individuals continued to load cash onto the cards over a number of weeks until they reached the account limit of $25 000 (AUSTRAC 2008 — case study 37).

The movement of funds internationally using debit cards and the ATM network is an established method of money laundering. Cards that allow access to the ATM network without the need for the cardholder to open a bank account or provide sufficient identification will create a greater risk of these cards being used for money laundering (FATF 2006).

Risks associated with closed system cards

Offenders perpetrating credit card fraud have been noted to purchase store gift cards using the fraudulently obtained credit card details. As noted in the *Organised fraud in Queensland* assessment (CMC 2009), a Malaysian organised crime group was found to have 42 gift cards worth about $13 000. These cards can often be purchased with no identification[42] and provide an easily portable and anonymous method of transporting the POC within Australia.

However, the risk of wider-scale money laundering using closed system cards such as store gift cards is considered lower than the risk with open system cards. Closed system cards tend to be available in smaller denominations and are often only honoured at a particular store or group of stores. Also, they are generally not able to be converted into cash or used to transfer value internationally.

CASE EXAMPLE 12

An individual was recently located with a number of false identity documents, $140 000 cash and 46 stored value cards. Further stored value cards and gift cards were located at the offender's premises. The cards appeared to be for values of between $50 and $500, and it is suspected that a number of the cards were purchased online (AUSTRAC 2008 — case study 42).

Law enforcement response

The AML/CTF Act includes the issuing of debit cards and stored value cards as designated services, and accordingly imposes reporting and AML/CTF program obligations on issuing entities. The Act defines debit cards as cards used to access an account held for the purposes of withdrawing or depositing cash, or obtaining goods or services.[43] The Act defines stored value cards as a portable device capable of storing monetary value in a form other than physical currency.[44]

Debit cards

The Act imposes reporting obligations, KYC obligations and OCDD obligations in relation to account holders and account signatories of debit card accounts.[45] These obligations should reduce the risk of accounts being opened and operated in false names, and also identify any unusual behaviour by account holders. The Act has also been framed in such a way that obligations regarding debit card services can be extended in the future to 'a person specified in the AML/CTF Rules'.[46] This provision should enable the Australian Government to respond to new providers of debit card services in Australia, and ensure they are bound by the AML/CTF framework.

42 No customer identification requirements are imposed by the AML/CTF Act if the value of the cards remains under threshold limits set out in the Act. These limits are discussed on page 26.

43 Refer to s. 5 of the AML/CTF Act and s. 63A of the *Trade Practices Act 1974* (Cwlth).

44 Refer to s. 5 of the AML/CTF Act.

45 These AML/CTF Act obligations are discussed in further detail below in the 'Law enforcement strategies' section.

46 Refer to s. 6, Table 1 — Items 18 to 20A (e) of the AML/CTF Act.

Stored value cards

The Act also imposes obligations regarding stored value cards where the cards reach certain dollar value thresholds. Reporting obligations, KYC obligations and OCDD obligations apply in relation to the person who is issued the card in the following instances:

- where any part of the value on the card can be withdrawn in cash, and the value on the card is $1000 or more, or can be increased to $1000 or more; or
- where no part of the value on the card can be withdrawn in cash and the value on the card is $5000 or more, or can be increased to $5000 or more.[47]

The Act has also allowed for these value thresholds to be amended by Regulation in the future.

Warning signs of money laundering

Debit cards and reloadable stored value cards

With respect to open system cards that can be used to access cash at ATMs, some money laundering warning signs for financial institutions include:

- use of false information or fraudulent documentation to open the account — particular attention should be paid to foreign and even interstate identification documentation
- structured cash deposits underneath the $10 000 reporting threshold
- transactions occurring at unusual locations that are inconsistent with the customer's usual profile
- cash deposits at Australian locations, and withdrawals at an overseas location, on a consistent basis (especially locations that are known tax havens or sources of illegal drugs)
- requests for multiple cards to access the account
- mailing addresses for replacement or new cards that are inconsistent with the location where the account was opened.

Non-reloadable stored value cards

With respect to closed system cards that cannot be reloaded or redeemed for cash, some money laundering warning signs are:

- multiple cards in possession of an individual
- receipts for the purchase of multiple cards.

Debit card and stored value card accounts with high-risk indicators such as those listed above need to be taken into account by reporting entities when assessing the risk of an account under their AML/CTF program. These accounts may require additional KYC and OCDD checks as specified in the AML/CTF Act, and the submission of suspicious matter reports to AUSTRAC.

47 Refer to s. 6, Table 1 — Items 21 to 24 of the AML/CTF Act.

4: Law enforcement strategies

This chapter discusses the effect of proceeds of crime legislation and the implications of the AML/CTF Act for money laundering in Australia.

Proceeds of crime

The *Criminal Proceeds Confiscation Act 2002* (Qld) (CPC Act) commenced on 1 January 2003. The Act contains two separate schemes for the recovery of the POC. One scheme is essentially a re-enactment of the predecessor conviction-based legislation and the second is a new non-conviction-based scheme commonly referred to as the civil confiscation scheme. The Act has equipped Queensland law enforcement with a useful tool for targeting the POC generated by Queensland offenders.

The Act introduced an innovative scheme for Queensland in the form of the non-conviction-based scheme. This scheme is administered by the Crime and Misconduct Commission (CMC) with the Director of Public Prosecutions appointed as the solicitor on the record. The Queensland Police Service (QPS) provides the majority of proceeds of crime litigation referrals. There has been a lot of activity under this new scheme to date, yet many provisions of the legislation still remain untested. At this time, only one matter has been fully litigated. Most matters are settled based on the financial and other evidence submitted by CMC and QPS investigators.[48] Figure 7 shows the value of property restrained and the number of restraining orders obtained since the inception of the Act.

Figure 8 on page 28 shows the amount of funds realised by the state and the number of matters settled since the commencement of the CPC Act.

To the end of the first quarter of 2008–09, Queensland had restrained in excess of $77 million and realised in excess of $14 million. It should be noted that, when the property of an offender is restrained, it severly restricts how this property is dealt with by the offender. That is, the restrained property is removed from the criminal environment and precluded from being used to further other criminal activity. Accordingly, there is an immediate value to the general public and law enforcement through criminal enterprises being limited when property is restrained. This benefit is subsequently obtained permanently when property is forfeited to, or realised by, the state.

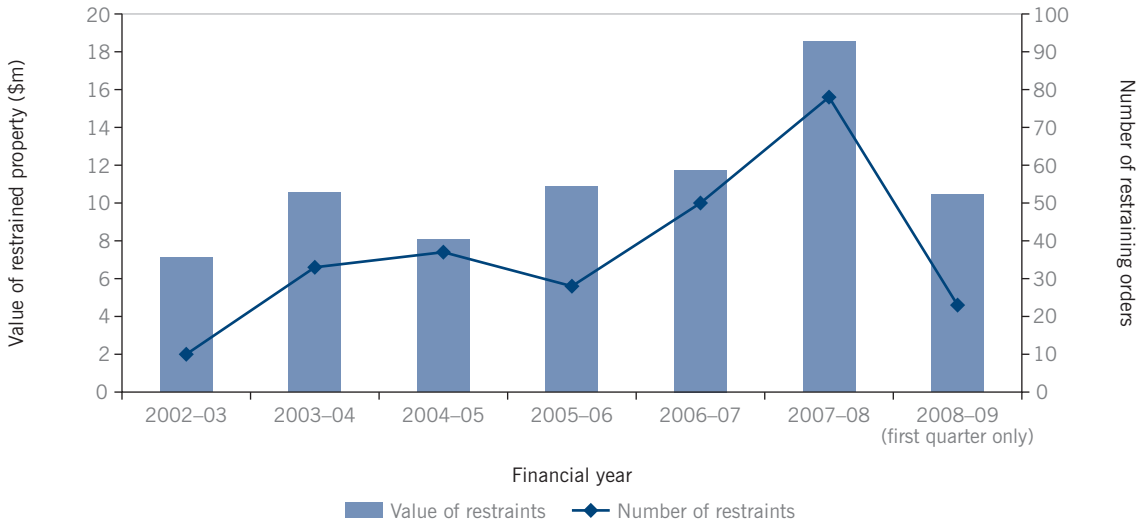
The increasing value of property restrained in the 2007–08 and 2008–09 financial years is strongly attributed to the increase in the number of proceeds of crime referrals from the QPS to the CMC. The upward trend in referrals is likely to be caused by the better integration of POC recovery into investigative practices. It is expected that the levels of POC that are restrained and realised will continue to grow in line with an increase in awareness of the civil confiscation scheme among QPS investigators and greater integration of POC recovery into investigation strategies.[49]

Although the number of proceeds of crime referrals has increased in recent times, there is scope for this to continue further if greater levels of financial investigative resources are

48 Discussions with CMC Proceeds of Crime Team, January 2009.

49 Ibid.

Figure 7: Property restrained under the CPC Act



available to the QPS. At present, in excess of 90 per cent of proceeds matters are linked to drug-related crime. In contrast, the restraining orders obtained by the Commonwealth Director of Public Prosecutions (CDPP) show that proceeds of crime litigation is predominantly linked to fraud-related offences (CDPP 2008). The value and number of restraining orders obtained in 2007–08 by various offence types are shown in Figure 9 (CDPP 2008).

There is no legislative impediment in Queensland to POC recovery in relation to fraud offences. However, recovery of proceeds under the CPC Act may impede the ability of victims to recover their losses through restitution orders, as the POC confiscated under the CPC Act are returned to consolidated revenue. It should also be noted that the Commonwealth POC figures have a higher fraud component because of proceeds of crime litigation against persons who have fraudulently obtained a range of Australian Government financial benefits.

The Anti-Money Laundering and Counter-Terrorism Financing Act

Background

In 2006, the Australian Government enacted the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). It is not the intention of this assessment to give a detailed overview of the AML/CTF Act, but it is worth noting how the implementation of the Act increases the robustness of Australia's anti–money laundering regime.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) reports that the AML/CTF Act contributes to the following goals:

- enabling Australia's financial sector to maintain international business relationships
- preventing and detecting money laundering and terrorism financing by meeting the needs of law enforcement

Figure 8: Proceeds of crime recovered

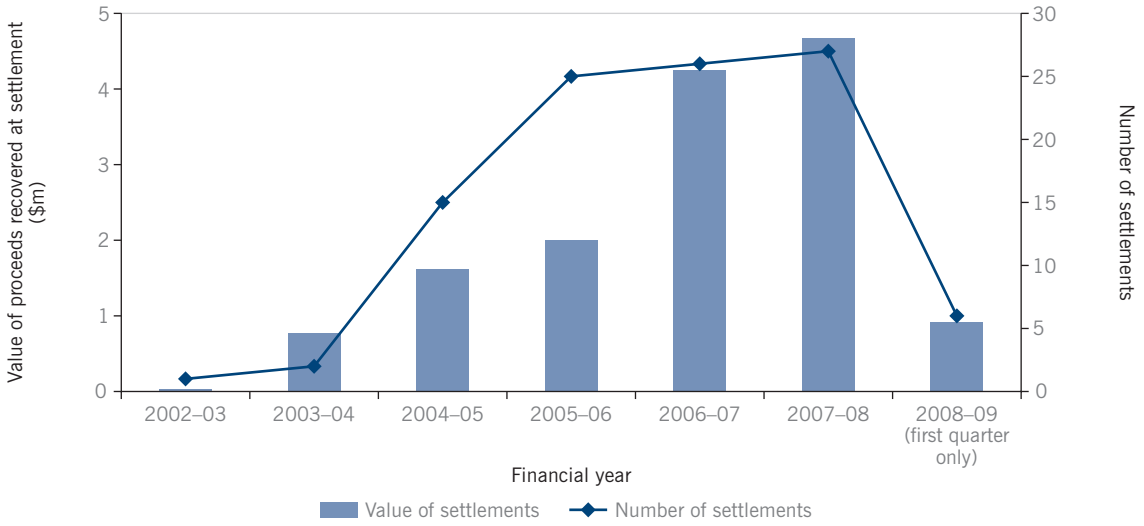
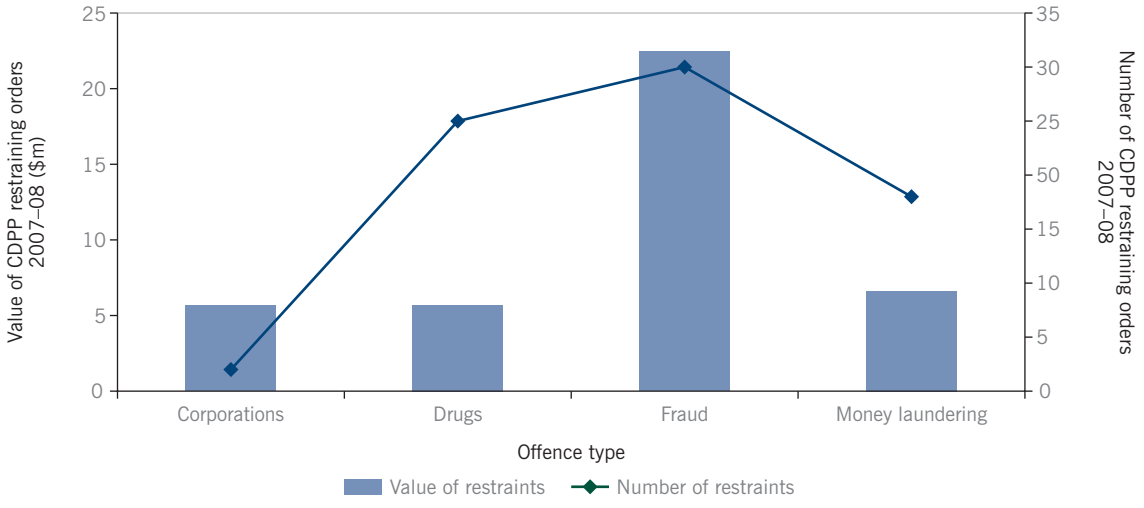


Figure 9: CDPP restraining orders by offence type



agencies for targeted information about possible criminal activity

- bringing Australia into line with international standards, including standards set by the Financial Action Task Force (FATF).

The AML/CTF Act builds on the financial compliance regime that was previously encompassed by the FTR Act. The changes implemented by the AML/CTF Act reflect Australia's response to revised international standards issued by the FATF on money laundering and terrorism financing. The FATF is an intergovernmental body whose purpose is to set international standards and develop policies to combat money laundering and terrorist financing.

Increased obligations of the AML/CTF Act

The FTR Act requires entities that satisfy the definition of a 'cash dealer' to report suspicious transactions, cash transactions of A$10 000 or more, and international funds transfer instructions to AUSTRAC. The FTR Act also requires cash dealers to verify the identity of persons who are signatories to accounts. Further, the FTR Act requires individuals to report cross-border movements of physical currency amounting to A$10 000 or more to AUSTRAC. The AML/CTF Act continues these obligations; however, it adopts a different approach to defining which entities are bound to adhere to them.

The AML/CTF Act has widened the net in terms of the institutions and businesses required to report to AUSTRAC. Although, in effect, the same reports exist (but with some slightly different names), the reporting obligation has been placed on entities that provide a 'designated service' as defined in s. 6 of the AML/CTF Act. That is, the Act focuses on the designated service provided as opposed to the definition of the institution. The Act also requires reporting entities to establish an AML/CTF program to minimise the risk of money laundering or terrorism financing activities being perpetrated within their organisation. It is expected that the changes in reporting requirements under the AML/CTF Act will also yield more informative and comprehensive data on reported transactions, which will provide LEAs with intelligence to better progress and initiate investigations.[50]

The AML/CTF Act imposes certain obligations on reporting entities when they provide designated services. Some of these obligations are:

- customer identification and verification of identity — by 12 December 2007
- record-keeping obligations — imposed throughout 2007
- establishment and maintenance of an AML/CTF program — by 12 December 2007
- ongoing customer due diligence and reporting (suspicious matters, threshold transactions and international funds transfer instructions) — by 12 December 2008.[51]

The AML/CTF Act also imposes an additional cross-border obligation not previously covered by the FTR Act. The Act now requires that a person must declare whether they are carrying BNIs in or out of Australia.[52] However, this obligation only arises if an individual is specifically asked about BNIs by a police officer or a customs and border protection officer. As noted earlier, the definition of a BNI does not include a stored value card or a debit card.[53]

Suspicious matter reports

The AML/CTF Act imposes obligations on reporting entities to submit suspicious matter reports (SMRs) in certain instances. These reports are likely to replace, to a large degree, the existing reports of suspect transactions (SUSTRs) under the FTR Act. However, the obligation to make SUSTRs under the FTR Act still exists. Reporting entities will be required to submit SMR reports in a wider range of circumstances than that encompassed by SUSTRs under the FTR Act.

Ongoing customer due diligence

It is expected that the Act will have an impact on money laundering through the imposition of ongoing customer due diligence (OCDD) requirements. Entities will need to continually monitor customers and their transactions. These requirements will help entities to mitigate the risk of money laundering by identifying unusual transactions or changes in customer behaviour.

The AML/CTF Rules specify three mandatory components of OCDD:[54]

1. **Collection and verification of additional know-your-customer (KYC) information**

   Although entities will collect and verify customer identification information before they provide services, they must also determine whether they need to obtain further KYC information or conduct additional verification during their relationship with this customer.

50 Discussions with CMC Proceeds of Crime Team, March 2009.

51 AUSTRAC 2009, viewed 30 January 2009, <www.austrac.gov.au/aml_ctf.html>.

52 See s. 200 of the AML/CTF Act.

53 A BNI is defined in s.17 of the AML/CTF Act as a bill of exchange, cheque, promissory note, bearer bond, traveller's cheque, money order, postal order or similar order or another negotiable instrument not covered by any of the above.

54 AUSTRAC 2009, viewed 30 January 2009, <www.austrac.gov.au/ongoingcustomerduediligence.html>.

2. **Transaction monitoring program**

   This forms part of an entity's overall AML/CTF program. It is designed to help entities to detect complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose. An entity may use software to flag such transactions when they fall outside a customer's usual activity.

3. **Enhanced customer due diligence program**

   In the event that an entity determines that there is a high money laundering (or counter-terrorism) risk, or that an account or customer has engaged in suspicious activity, the entity must consider whether it needs to verify or update KYC information, further analyse and monitor customer transactions or submit a suspicious matter report to AUSTRAC.

As seen in some of the money laundering examples discussed earlier, customers can become mules for money launderers and start receiving and remitting money overseas. Alternatively, a bank customer who is the genuine recipient in a cuckoo smurfing scheme may receive unusual deposits that are structured, lump cash sums or deposits at locations not usually used by the customer. It is these types of atypical behaviour which should be detected through OCDD monitoring and subsequently reported to AUSTRAC. These focused monitoring obligations should be beneficial in the fight against money laundering in a number of ways — offenders will be dissuaded from certain money laundering activities, and the associated reporting through AUSTRAC will provide valuable intelligence to law enforcement agencies to progress or initiate investigations into money laundering.

In summary, the additional obligations and extended coverage of reporting entities captured by the AML/CTF Act should make it more difficult for offenders to launder the POC. In addition, the changes should reduce the extent of accounts operated and transactions conducted in false names. These additional KYC requirements should also assist in combating identity fraud. However, the problems that remain are how to ensure compliance by reporting entities, and the use of non-compliant entities by organised crime groups to conduct transactions and remit funds.

A second tranche of the AML/CTF Act is also proposed which will widen the designated services to which AML/CTF obligations apply. The sectors likely to be affected by the second tranche of legislation are:

- real-estate agents in relation to buying and selling of properties
- dealers in precious metals and stones engaged in transactions above a designated threshold
- lawyers, notaries, other independent legal professionals and accountants when preparing for or carrying out certain transactions
- trust and company service providers when they prepare for or carry out for a client the transactions listed in the glossary to the FATF recommendations.[55]

55 AUSTRAC 2009, viewed 30 January 2009, <www.austrac.gov.au/aml_ctf.html>. Details of proposed additional designated services are listed in a table at the following location (viewed 30 January 2009): <www.austrac.gov.au/files/second_tranche_designated_services_tables.pdf>.

5: Risk assessment methodology

This chapter assesses the level of risk to the Queensland community posed by money laundering perpetrated by organised crime networks.

THE RISK ASSESSMENT MATRIX IS ESSENTIALLY A SERIES OF FORMULAE TO DETERMINE LEVEL OF RISK
Desire × confidence = intent
Resources × knowledge = capability
Intent × capability = likelihood of threat
Likelihood of threat × harm / consequences = RISK

Risk =	Negligible	Very low	Low	Medium	High	Very high	Certain

The risk of money laundering in Queensland is assessed as **HIGH**. We calculated this as follows:

Intent

The *INTENT* is assessed as **HIGH**. This relates to the desire and confidence of organised offenders. Organised groups have a strong desire to launder their proceeds of crime (POC) in order to avoid confiscation litigation and enjoy the fruits of their labour. The implementation of civil-based confiscation legislation in Queensland and elsewhere in Australia has resulted in a greater incentive for offenders to distance themselves from or legitimise their POC. The confidence of organised groups in carrying out money laundering activities is bolstered by their use of third parties to assist in the money laundering process. For example, offenders have used mules to move the proceeds of fraud offences, and third parties in schemes such as cuckoo smurfing. The use of alternative remittance systems (ARSs) has also provided offenders with a level of anonymity which further contributes to their confidence in carrying out money laundering activities.

Capability

The *CAPABILITY* is assessed as **HIGH** and relates to the knowledge and resources available to organised crime networks. From the more intricate examples of money laundering that have been noted, offenders have accessed international money remitters, corporate structures and bank accounts in their own and third-party names, to conduct transactions and disguise the source of POC. The wide range of techniques used by organised groups displays the breadth of knowledge and inventiveness that organised groups employ to launder their tainted funds. As technology increases and global financial transactions become more widespread, the capability of offenders to exploit new financial products is also expected to increase. From discussions with the Australian Federal Police, investigators believe that, as the financial reporting regime changes, money laundering methodologies will change accordingly.[56]

Threat

The *THREAT* is assessed as **HIGH**, given that it is a function of intent (HIGH) and capability (HIGH).

The *HARM* is assessed as **HIGH** because of the financial costs associated with anti-money laundering compliance. These costs include the high cost to institutions classed as 'reporting entities' under the AML/CTF Act in implementing mandatory AML/CTF programs and carrying out additional responsibilities associated with ongoing customer due diligence. In a study conducted in 2008, the cost of implementation of the AML/CTF regime for the Australian banking industry was estimated to be $1.02 billion (Sathye 2008).

There is also a high cost to the Australian Government in monitoring compliance with the AML/CTF Act, public awareness campaigns, and maintaining databases to record and store the expected increasing number of financial reports submitted by 'reporting entities'.

56 Discussions with AFP Brisbane, October 2008.

The Australian Government's increase in appropriations to fund anti–money laundering and counter-terrorism financing reforms can be seen in the appropriation funding until 2010 for the Australian Transaction Reports and Analysis Centre (AUSTRAC), which is as follows:

- 2006–07: $36.693 million
- 2007–08: $59.274 million
- 2008–09: $54.928 million
- 2009–10: $56.136 million (PJC–ACC 2007).

In a submission by AUSTRAC to the Parliamentary Joint Committee on the Australian Crime Commission (PJC–ACC) in 2007, it was noted that money laundering causes financial harm to legitimate small businesses because of the unfair business advantage for businesses that are laundering money (PJC–ACC 2007).

An additional area of harm has been noted by the PJC–ACC, namely that the removal from the country of large sums of illicitly obtained Australian currency undermines the assets, liabilities and operations of financial institutions. Also, tax revenue is lost as a result of money laundering activities, which in turn undermines the provision of government services (PJC–ACC 2007).

In summary, money laundering can be seen to impose significant costs on the government, small businesses and financial institutions. Also, the additional costs to financial institutions are likely to be passed on to the Australian public through increased banking fees.

Risk

The *RISK* is therefore assessed as **HIGH**, as it is a function of threat (HIGH) and harm (HIGH).

Intent	Capability	Threat	Harm	Risk
HIGH	**HIGH**	**HIGH**	**HIGH**	**HIGH**

References

ACC — *see* Australian Crime Commission.

AFP — *see* Australian Federal Police.

APG — *see* Asia/Pacific Group on Money Laundering.

Asia/Pacific Group on Money Laundering 2008, *APG typologies report 2008, 11 July 2008*, viewed 14 January 2009, <www.apgml.org/documents/docs/6/APG_2008_Typologies_Rpt_July08.pdf>.

AUSTRAC — *see* Australian Transaction Reports and Analysis Centre.

Australian Crime Commission 2007, submission to the Parliamentary Joint Committee on the Australian Crime Commission Inquiry into the Future Impact of Serious and Organised Crime on Australian Society.

Australian Federal Police 2008, *Intelligence brief: criminal use of prepaid cards*, 19 May 2008.

Australian Transaction Reports and Analysis Centre 2007a, *The extent of money laundering in and through Australia in 2004*, viewed 19 January 2009, <www.aic.gov.au/crc/reports/200304-33.html>.

—— 2007b, *Typologies and case studies report 2007*, viewed 25 February 2009, <www.austrac.gov.au/files/typologies_report.pdf>.

—— 2008, *Typologies and case studies report 2008*, viewed 20 January 2009, <www.austrac.gov.au/files/austrac_typologies_2008.pdf>.

Camdessus, M 1998, 'Money laundering: the importance of international countermeasures', address at the Plenary Meeting of the Financial Action Task Force on Money Laundering, Paris, France, viewed 31 January 2009, <www.imf.org/external/np/speeches/1998/021098.htm>.

CDPP — *see* Commonwealth Director of Public Prosecutions.

Choo, R 2008, *Money laundering risks of prepaid stored value cards*, Australian Institute of Criminology Trends & Issues no. 363, September 2008.

CMC — *see* Crime and Misconduct Commission.

Commonwealth Director of Public Prosecutions 2008, *Annual report 2007–08*, viewed 31 January 2009, <www.cdpp.gov.au/Publications/AnnualReports/CDPP-Annual-Report-2007-2008.pdf>.

Crime and Misconduct Commission 2004, *Organised crime markets in Queensland: a strategic assessment*, Crime Bulletin Series, no. 6, Crime and Misconduct Commission, Brisbane, September.

—— 2009, *Organised fraud in Queensland: a strategic assessment*, Crime and Misconduct Commission, Brisbane.

FATF — *see* Financial Action Task Force.

Financial Action Task Force 2005, *Money laundering and terrorist financing typologies 2004–2005*, 10 June 2005.

—— 2006, *Report on new payment methods*, 13 October 2006.

Flatley, C 2008, 'Money laundering "mule" jailed', *Age*, 12 February 2008, viewed 16 January 2009, <news.theage.com.au/national/money-laundering-mule-jailed-20080212-1rrf.html>.

Lutton, E 2008, 'Outlaw bikies snatch money trade: lender', Sun Herald, 21 December 2008, p. 4.

National Drug Intelligence Centre 2006, *Assessment: prepaid stored value cards: a potential alternative to traditional money laundering methods*, 31 October 2006, viewed 3 February 2009, <www.usdoj.gov/ndic/pubs11/20777/index.htm>.

NDIC — *see* National Drug Intelligence Centre.

Parliamentary Joint Committee on the Australian Crime Commission 2007, *Inquiry into the future impact of serious and organised crime on Australian society*, September 2007, viewed 19 January 2009, <www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/2004-07/organised_crime/report/report.pdf>.

PJC–ACC — *see* Parliamentary Joint Committee on the Australian Crime Commission.

Rout, M 2008, 'Innocent bank clients used to launder drug cash via "cuckoo smurfing"', *Australian*, 22 August 2008, viewed 29 January 2009, <www.theaustralian.news.com.au/story/0,25197,24221712-2702,00.html>.

Sathye, M 2008, 'Estimating the cost of compliance of AMLCTF for financial institutions in Australia', *Journal of Financial Crime*, vol. 15, no. 4, pp. 347–63.

Serious Organised Crime Agency 2008, *United Kingdom threat assessment of serious organised crime 2008/9*, March 2008.

SOCA — *see* Serious Organised Crime Agency.

Tipper, D 2007, 'Payday lenders won't wear interest cap', Australian Broadcasting Corporation, 19 October 2007, viewed 14 January 2009, <www.abc.net.au/local/stories/2007/10/19/2063904.htm>.

Tung, L 2008, *Real-life internet scammers dissected*, ZDNet Australia, 5 November 2008, viewed 20 January 2009, <www.zdnet.com.au/insight/security/soa/Real-life-internet-scammers-dissected/0,139023764,339292871-1,00.htm>.

Viellaris, R 2008, 'Dirty money laundered at casinos by welfare recipients', *Courier-Mail*, 5 December 2008, viewed 5 February 2009, <www.news.com.au/couriermail/story/0,23739,24757508-952,00.html>.

Walker, J 1995, *Estimates of the extent of money laundering in and through Australia: prepared for the Australian Transaction Reports and Analysis Centre*, AUSTRAC, Canberra.

Legislation cited in this assessment

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cwlth)

Casino Control Act 1982 (Qld)

Consumer Credit (Queensland) Act 1994

Consumer Credit (Queensland) Special Provisions Regulation 2008

Crime and Misconduct Act 2001 (Qld)

Criminal Proceeds Confiscation Act 2002 (Qld)

Criminal Proceeds Confiscation and Other Acts Amendment Act 2009 (Qld)

Drugs Misuse Act 1986 (Qld)

Financial Transaction Reports Act 1988 (Cwlth)

Police Powers and Responsibilities Act 2000 (Qld)

Proceeds of Crime Act 2002 (Cwlth)

Trade Practices Act 1974 (Cwlth)

About the Crime Bulletin

The CMC publishes Crime Bulletins to heighten community awareness of organised crime issues and trends of concern to the Queensland community.

Previous issues in the Crime Bulletin series are:

- Crime Bulletin no. 10, October 2009, *Organised fraud in Queensland: a strategic assessment*, which provides an overview of current and emerging issues relating to online, credit card, identity and cheque fraud.
- Crime Bulletin no. 9, June 2009, *Organised property crime markets in Queensland: a strategic assessment*, which describes the nature and extent of organised property crime markets in Queensland.
- Crime Bulletin no. 8, September 2007, *The cocaine market in Queensland: a strategic assessment*, which examines current trends and issues for cocaine use and the status of the market in Queensland.
- Crime Bulletin no. 7, December 2005, *Property crime in Queensland: a strategic assessment*, which examines the property crime market in Queensland, primarily to reveal the nature and extent of organised criminal activity within this environment.
- Crime Bulletin no. 6, September 2004, *Organised crime markets in Queensland: a strategic assessment*, which describes the organised crime landscape and discusses the main illicit markets that drive organised criminal activity in Queensland.
- Crime Bulletin no. 5, June 2003, *Amphetamine: still Queensland's no. 1 drug threat*, which provides a strategic assessment of the illicit amphetamine market in Queensland, based on an analysis of a diverse range of sources including information from law enforcement, government, industry and members of the community.
- Crime Bulletin no. 4, April 2002, *The illicit market for ADHD prescription drugs in Queensland*, which discusses the problem of illicit diversion and abuse of ADHD prescription drugs in Queensland.
- Crime Bulletin no. 3, August 2001, *The 'ecstasy' market in Queensland*, which assesses the level of risk posed to the Queensland community by the market for MDMA or ecstacy.
- Crime Bulletin no. 2, November 2000, *The amphetamine market in Queensland*, which assesses the level of risk posed to the Queensland community by the illicit amphetamine market.
- Crime Bulletin no. 1, June 1999, *Organised crime in Queensland*, which describes the nature, extent and impact of organised crime activity in Queensland, and generally explains the law enforcement strategies developed to tackle the problem.

These bulletins and other CMC publications can be viewed on the CMC's website <www.cmc.qld.gov.au>.

CRIME AND MISCONDUCT COMMISSION

QUEENSLAND