CRIME BULLETIN

CRIME AND MISCONDUCT COMMISSION QUEENSLAND

CRIME BULLETIN SERIES

NUMBER 10, OCTOBER 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

Organised fraud in Queensland

A strategic assessment

Summary

Our 2009 fraud assessment focuses on major organised crime groups and their use of fraud both as a means to earn money and as a facilitator of further criminal enterprise. Although many fraud offences are opportunistic and carried out by individuals or groups, our assessment focuses on fraud committed by organised criminal networks against persons, businesses and companies; it does not extend to corporate sector fraud.

This summary provides an overview of current and emerging issues relating to online, credit card, identity and cheque fraud.

Online fraud

Background of online fraud

With the advances in technology, online fraud has proliferated and many organised crime networks have been encouraged to become involved. According to internet security company McAfee (2006, p. 2), 'cybercrime represents the fastest-growing category of crime globally'.

In the last decade, internet use has significantly increased as a means of communicating, accessing information and undertaking commerce. The internet has many benefits for users, including convenience, speed, accessibility and cost-effectiveness. Between 2001 and 2008, internet usage by Australian consumers more than doubled, from 35 per cent of the population (ABS 2006) to 74 per cent (Internet World Stats).

Improvements in technology and an increase in electronic storage, transmission and sharing of data have made online crimes easier to commit and harder to detect (ABS 2008; Walters & Galvin 2008). Increased internet usage by Australians has led to an increased exposure to online fraud. Individuals and organisations have become so reliant on computers to store, communicate and process information that vast opportunities have been created for these technologies to be misused.

In 2008, Australia was the sixth most targeted country in the world for Trojan attacks (Chia Fei, cited in Walters & Galvin 2008) and about one in six Australian home computers were compromised (Walters 2008a). It has been suggested that an unprotected computer with an internet connection may be compromised by malicious software (see Glossary) in as little as four minutes.

Black-market web portals

Many fraud offenders rely on black-market web portals (BMWPs) to conduct training modules, to discuss new methodologies and vulnerabilities, and to trade viruses, mailing lists, spamming tools and personal, financial and identity information (*Sydney Morning Herald* 2008; Walters 2008b). It is not known how many BMWPs exist, but it is likely that as soon as law enforcement shuts one down others reappear in its place.

Phishing

Consumers are more aware of phishing attacks (see Glossary) and this may explain why only 0.4 per cent of people fell victim to phishing scams in 2007 (ABS 2008). Fraud offenders are moving away from the typical 'update your banking details' emails to more varied and directed messages (McAfee 2006).

Advance fee fraud

In Queensland, the effects of advance fee fraud (AFF), such as Nigerian scams (see Glossary), have been such that the Queensland Police Service (QPS) has introduced several initiatives in a bid to reduce the number of victims of these schemes and the amount of money lost to them. Australians, in general, are continuing to fall victim and are losing millions each year as a result. Members of the community facing financial struggles as a result of the current global financial crisis may be more susceptible to 'get rich quick' schemes. People who otherwise would not be taken in by AFFs may become victims when they are under financial pressure.

Summary of online fraud

The internet and technology have significantly assisted organised criminal networks to fraudulently obtain personal details and information to use for their benefit. Dependence by the wider population on information techology has meant that methodologies used by criminals are evolving to include this technology as part of their offending. Organised criminal networks may be driven to offend online because the internet provides anonymity, security, a high return for a relatively low risk and a global network in which to target victims.

There do not appear to be sophisticated criminal groups operating from within Queensland. However, Queenslanders are significantly affected financially and emotionally by online fraud conducted nationally and globally by organised networks.

Credit card fraud

According to figures released in 2007 by the Australian Payments Clearing Association, there were 43 million plastic debit and credit cards on issue to Australians in 2007 — this equates to about 2.5 cards for every Australian over 18 years of age. Since the financial year 1994–95, the number of credit card accounts has remained relatively stable, but the number of transactions conducted on these cards has increased exponentially (Reserve Bank of Australia). The more transactions that are conducted, the greater the chance of that information being captured and used by fraud offenders.

Acronyms

ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
AFF	advance fee fraud
AHTCC	Australian High Tech Crime Centre
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth)
APACS	Association for Payment Clearing Services (UK)
APCA	Australian Payments Clearing Association
ATM	automatic teller machine
AusCERT	Australian Computer Emergency Response Team
BMWP	black-market web portals
CM Act	*Crime and Misconduct Act 2001*
CMC	Crime and Misconduct Commission
DCITA	Department of Communications, Information Technology and the Arts
DFAT	Department of Foreign Affairs and Trade
EFTPOS	electronic funds transfer at point of sale
ICT	information and communication technology
IT	information technology
OSCA	Office of Strategic Crime Assessments
PIN	personal identification number
PED	PIN entry devices
QPRIME	Queensland Police Records and Information Management Exchange
QPS	Queensland Police Service
RBDM	Registry of Births, Deaths and Marriages
SIM	subscriber identification module
SOCA	Serious Organised Crime Agency

Acknowledgments

In preparing this report, officers of the Crime and Misconduct Commission consulted with the Queensland Police Service, Queensland Casinos, various financial institutions, credit unions and building societies, Australian Computer Emergency Response Team, the Office of Fair Trading, the Australian Crime Commission, the Australian Federal Police, the Australian Customs and Border Protection Service, the Australian Institute of Criminology, the Australian High Tech Crime Centre and the Australian Transaction Reports and Analysis Centre. The CMC wishes to acknowledge the valuable assistance provided by these agencies and their officers.

The CMC's Strategic Intelligence Unit was responsible for writing this report and conducting the analyses presented, but would like to acknowledge the assistance provided by other areas of the organisation in completing the report.

The report was prepared for publication by the Communications Unit.

A criminal market in stolen credit card details has been able to flourish, as a result of:

- the numerous ways in which credit card details can be obtained
- the affordability of purchasing card details
- the anonymity provided by the internet
- the ability of criminals to easily enter the market.

Attempts to obtain the data contained on credit card strips has been, and will continue to be, exploited by hackers and organised fraud offenders, particularly for 'card-not-present' transactions.

Money mules

Increasingly, people are being recruited by fraud offenders to act as 'money mules' (see Glossary) to forward stolen money that has been sent to their bank account. Mules are recruited through employment advertisements for positions such as international sales representatives or shipping managers (Crawford 2008). These job advertisements may be placed on employment websites or may be spam advertisements sent by email. Fraud offenders use the brand names of well-known organisations, and have been known to create false websites and establish email addresses linked to the false website, so as to appear legitimate.

Money muling is an organised criminal activity and has been identified in Queensland. It is assessed that the use of money mules will increase because of the current downturn in the economy. Organised fraud offenders are taking advantage of cash-strapped employment seekers (Crawford 2008). Even people who would not normally be lured into money-muling activities, may now consider it because it affords a relatively easy way to earn money. Furthermore, people desperate for employment are less likely to ask questions about the legitimacy of the employment.

Card skimming

According to QPS statistics, the discovery of skimming devices (see Glossary) in Queensland has reduced. This could have been for a number of reasons:

- the QPS was not advised by financial institutions when skimmers were discovered attached to their ATMs
- the risks associated with importing a skimmer into Australia and having to install it were a deterrent to potential offenders
- the ease with which credit card dumps (see Glossary) could be purchased online, and the low cost of the dumps, made this method of offending a more attractive option than skimmers
- skimmers remained undetected until such time as the victim's card details were used in another location, by which time the device had been removed and was unable to be recovered.

Glossary

Advance fee fraud
Scams aimed at persuading a victim to send an amount of money by making them believe that by doing this they will eventually receive a lot more.

Credit card dumps
A dump of information contained on bank cards' magnetic strips. This includes the card's account number, expiry date and credit card verification number.

Fraud offenders
A generic term used throughout this assessment to describe any person or persons involved in committing an offence of fraud.

Malicious software (malware)
Computer code that is secretly placed onto a person's computer allowing information about that person to be sent back to a third party or to cause harm to their system or other systems.[1] Malware can infect a computer through an email with the virus attached, through an email with a link in the body of the email that when clicked activates the malware, or through a victim visiting a compromised website.

Money mules
Money mules are people who are recruited to receive sums of money into their account and are then required to forward this money back to the organisers of the fraud. Often fraud offenders entice people to work for them as mules by advertising positions of employment.

Phishing
Phishing is an attempt to obtain a person's personal details, such as account numbers, passwords and credit card details. Phishing can take a variety of forms, including email, phone, post or in person.

Skimming device
A device that is attached to automatic teller machines (ATMs) or to merchant terminals in stores, and records the contents of a bank card's magnetic strip. Such information includes the card's account number, expiry date and credit card verification number.

1 Australian Communications and Media Authority website, 2007, and Organisation for Economic Co-operation and Development 2008.

In an attempt to combat card skimming, several systems are being introduced in Australia, such as chip and personal identification number (PIN) technology and 'jitters' (explained further on page 16).

Identity fraud

Advances in technology have made it easier for organised criminal groups to obtain personal information to create legitimate-looking fraudulent documents. Improvements in the quality of scanning equipment, photocopiers, printers and digital image manipulation software have assisted with this (SOCA 2008).

Amendments to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth) (AML/CTF Act) no longer require customers to show '100 points' of identification when opening accounts, although it is likely that many financial institutions will continue to rely on this. With the introduction of policies such as 'ongoing customer due diligence', reporting entities are required to monitor and 'know' their customers. This may affect identity fraud in that mules may have to attend more financial institutions than previously or handlers may have to recruit more mules.

Several initiatives have been, or will soon be, implemented with the aim, in part, of reducing identity fraud:

- *Queensland smartcard driver licences* — A computer chip will be embedded in these licences to digitally store personal information, in an attempt to reduce counterfeit licences being produced, and to identify people holding several licences in different names.
- *The Australian ePassport using biometrics* — Biometrics are considered an effective method for security and identification purposes. Although the use of biometrics may be costly to implement and maintain, the cost is decreasing (Zoica 2007), which will make biometrics a more viable option in the future.
- *Implementation of policies* — Under the AML/CTF Act, as mentioned above, implementation of new policies is an attempt to reduce indentity fraud.
- *Registry of Births, Deaths and Marriages (RBDM)* — The introduction of security certificate paper is also a new initiative.

Cheque fraud

Cheque fraud is on the decline. Although it still occurs, it is mainly conducted by opportunistic offenders who steal a chequebook while conducting a break and enter. The United Kingdom's Serious Organised Crime Agency in its 2006 threat assessment identified that attempts at cheque fraud had increased as a result of the introduction of chip and PIN technology. Given the experiences of the United Kingdom, this is an area that should be monitored as Australia comes closer to full implementation of chip and PIN cards.

Strategies

There are a number of strategies that may enhance the effectiveness of law enforcement efforts to reduce fraud in Queensland:

- public awareness of computer protection
- continued fostering of partnerships
- suspension of online banking accounts by financial institutions
- creation of a central reporting and strategic body.

Risk assessment

As identified in this 2009 assessment, the extent of fraud committed by organised criminal networks is limited primarily to online fraud and identity fraud (including credit card fraud). It is deemed that many of the 'street fraud' are committed by opportunistic individuals or groups and not by organised criminal networks. The risk of online fraud is assessed at the high end of MEDIUM. The involvement by organised criminal networks in online fraud is increasing and warrants monitoring. The risk of identity fraud, including credit card fraud, is assessed as HIGH. The involvement of organised criminal networks in identity fraud is increasing.

Structure of the report

This assessment of organised fraud in Queensland is presented in five chapters:

- **Chapter 1** discusses the background and scope of this assessment and explains the data collection and risk assessment methodologies used.
- **Chapter 2** describes the difficulties faced in accurately measuring fraud and details the nature and extent of fraud in Australia.
- **Chapter 3** explains the various types of fraud that has emerged or changed since the last CMC assessment, completed in 2004, and the involvement of organised crime groups in Queensland. The various types of fraud has been grouped into four different areas; however, many kinds of fraud are interrelated.
- **Chapter 4** assesses the current organised fraud market in Queensland, examines the level of risk to the Queensland community posed by organised fraud networks, and outlines proposed strategies aimed at assisting the investigation and reduction of fraud in Queensland.

1: Introduction

This chapter discusses the background and scope of this assessment and explains the data collection and risk assessment methodologies that have been used.

Background

Our assessment follows on from two previous strategic assessments compiled in 1999 and 2004. The first assessment of crime markets was a joint project known as Project Krystal, conducted by the then Queensland Crime Commission (QCC) and the Queensland Police Service (QPS). 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. The assessment concluded that the risk posed by fraud was HIGH.

In 2004, the Crime and Misconduct Commission (CMC) compiled the document *Organised crime markets in Queensland: a strategic assessment*. This assessment not only provided an update on the status of markets since the first assessment in 1999, but also identified further markets into which organised crime networks had moved.

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

The aim of this assessment is to:

- determine if there has been a shift in fraud perpetrated by organised criminal networks, as opposed to fraud by individuals
- describe the characteristics of specific types of organised fraud
- assess the risk posed by major identified types of organised fraudulent activity
- recommend strategies to help individuals and corporations prevent and avoid fraud risks
- identify the nature of and trends in identity crime, and suggest prevention strategies
- analyse how identity crime facilitates fraud and determine the extent of identity crime perpetrated by organised groups.

Scope of this paper

This paper focuses on offences committed against persons, businesses and companies by organised criminal networks. The assessment does not focus on corporate sector fraud committed by employees against their employer, the defrauding of shareholders by directors and company officers, insurance fraud, or the defrauding of Commonwealth agencies such as Centrelink or the Australian Taxation Office.

Fraud has been defined according to s. 408C of the *Criminal Code Act 1899*, which states:

(1) A person who dishonestly —

(a) applies to his or her own use or to the use of any person —

(i) property belonging to another; or

(ii) property belonging to the person, or which is in the person's possession, either solely or jointly with another person, subject to a trust, direction or condition or on account of any other person; or

(b) obtains property from any person; or

(c) induces any person to deliver property to any person; or

(d) gains a benefit or advantage, pecuniary or otherwise, for any person; or

(e) causes a detriment, pecuniary or otherwise, to any person; or

(f) induces any person to do any act which the person is lawfully entitled to abstain from doing; or

(g) induces any person to abstain from doing any act which that person is lawfully entitled to do; or

(h) makes off, knowing that payment on the spot is required or expected for any property lawfully supplied or returned or for any service lawfully provided, without having paid and with intent to avoid payment;

commits the crime of fraud.

The extent of organisation

An organised criminal group is defined according to Schedule 2 of the *Crime and Misconduct Act 2001* (CM Act), which states that organised crime is an activity involving:

a. indictable offences punishable on conviction by a term of imprisonment not less than seven years; and

b. two or more persons; and

c. substantial planning and organisation or systematic and continuing activity; and

d. a purpose to obtain profit, gain, power or influence.

The 2004 CMC assessment of crime markets identified that most frauds are committed by individuals rather than by organised criminal networks (CMC 2004). With advances in technology, online fraud has proliferated and many organised crime networks have been encouraged to become involved. It is likely that the types of fraud that do not require information and communication technology (ICT) are still being conducted, in the majority, by opportunistic individuals and groups. ICT has allowed many organised crime networks to exploit online technologies to commit fraud.

Methodology

Data collection

Information for our assessment was obtained from a variety of sources. Semi-structured interviews/consultations were conducted with several government and law enforcement agencies and private organisations, and a review of the relevant literature was undertaken. Quantitative data of the Australian Payments Clearing Association (APCA), QPS reported data for the financial years 1998–99 to 2007–08 and data from the Reserve Bank of Australia (RBA), were also consulted.

Qualitative data

Information obtained during consultations with representatives of law enforcement agencies and other public and private sector organisations may have been affected by the following:

- Ability to recall details of events. This may be impaired by the passing of time or by the extent of involvement of the respondent in the event.
- Interviewer bias. It is possible that questions failed to target specific areas, questions were misunderstood or answers were misinterpreted.

Some of the information received during consultations was anecdotal. Attempts have been made to validate this information by verifying it against other sources such as intelligence holdings and reported crime data.

Quantitative data

QPS statistics of reported offences for the financial years 1998–99 to 2007–08 were consulted. These statistics may not be entirely accurate for the following reasons:

- QPS officers may have reported offences using incorrect crime classes.
- In 2007, new crime classes were introduced on the Queensland Police Records and Information Management Exchange (QPRIME). As a result, it is difficult to compare data pre-2007 and post-2007.
- QPS data relate only to offences reported to the QPS and do not provide a complete measure of the extent of fraud offences throughout Queensland.

It is difficult to quantify the extent of fraud offences occurring in Queensland. Much of the fraud data published relates to Australia as a whole, which makes it difficult to obtain information specific to Queensland.

2: The background to fraud

This chapter describes the difficulties faced in accurately measuring fraud and details the nature and extent of fraud in Australia.

Measuring fraud

Only during the last decade have research and survey instruments attempted to identify the nature and extent of fraud in Australia. The following surveys have all contributed to an understanding of the types of fraud present in Australia, their victims and community attitudes to fraud:

- the Australian Institute of Criminology's Crime Victims Survey (2000) and International Crime Victimisation Survey (2004)
- accounting firm KPMG's Fraud Survey (2006)
- the Australian Computer Emergency Response Team's (AusCERT) Australian Computer Crime and Security Surveys (2002–06) and the Home Users Computer Security Survey (2008).

In 2007, the Australian Bureau of Statistics (ABS) conducted its first survey on personal fraud.[2] The ABS identified that 25 per cent of the people who took part in the survey and who were victims of credit card fraud did not report the incident to either a bank or the police. Similarly, 43 per cent of people who were the victim of identity theft did not report the fraud to police or the issuer of the document.

The ABS found that the accuracy of statistics could be affected by factors such as:

- the ability of people to recall incidents that have occurred in the past
- the ability of people to make judgments about whether some of their experiences have been legitimate or fraudulent
- people's degree of willingness to reveal if they have been deceived or have incurred significant financial loss
- lack of awareness by people that they have been deceived or become victims of fraud (ABS 2008).

The true extent of fraud committed not only in Queensland but around the world is largely unknown. There is no practical way of assessing the prevalence of fraud simply because many incidents of fraud are not reported, properly identified or even detected by victims (Urbas & Choo 2008; Rollings 2008). Furthermore, official police statistics are not collected in a way that accurately reflects the extent of the situation and police services in each state and territory record offences differently.

Apart from reporting to the Queensland Police Service (QPS) and financial institutions, there are many government agencies to which victims of fraud can report, depending on the type of fraud. Such agencies include the Australian Consumer and Competition Commission, the Office of Fair Trading and the Australian Communications and Media Authority. These agencies record fraud complaints according to their own internal reporting mechanisms and, as a result, the data are often not comparable across agencies (Smith 2007a). There is also a risk of duplication of fraud figures if victims report the same matter to several agencies.

According to the 2006 KPMG Fraud Survey, which asked businesses what costs were incurred investigating their largest types of fraud, most businesses responded that approximately 25 per cent of the cost of the particular fraud was incurred in investigating it. Given that fraud costs so much to investigate, some businesses and companies may see it as not being worth their while to report offences. Furthermore, organisations such as banks factor in an annual amount of money that they will lose to fraud. This can blur the actual amount of money lost as a result of fraud.

The nature and extent of fraud

Bearing in mind the difficulties faced in accurately measuring the frequency of fraud in Australia, it has been suggested by the ABS (2008) that Australians lost close to $1 billion to personal fraud in 2007. This figure represented the losses incurred on debit and credit cards and online scams as a result of fraud.

The ABS fraud survey identified that 806 000 Australians (5 per cent) aged 15 years and over were the victims of personal fraud in the 12 months prior to interview for the July 2007 to June 2008 survey.[3] Of these victims, 329 000 (2 per cent) were victims of a scam and 499 500 were victims of identity fraud.[4] According to the KPMG 2006 Fraud Survey, there were 546 instances in Australia, totalling $2.8 million, where a person's identity was used fraudulently to obtain new loans (KPMG 2006).

2 The ABS national personal fraud survey (ABS 2008) was conducted between July 2007 and December 2007. Respondents were asked to recall incidents only in the 12 months prior to completing the survey. This survey was conducted in conjunction with the multi-purpose household survey (MPHS). The MPHS sample answered all the MPHS questions, including the personal fraud module.

3 Personal fraud for the purpose of the ABS survey included credit or bank card fraud, identity theft and scams including lottery scams, pyramid schemes, phishing, financial advice, chain letters and advance fee fraud.

4 Of the 499 500 people, 383 300 (2.4 per cent) were victims of credit or bank card fraud and 124 000 (0.8 per cent) were victims of identity theft. People who experienced fraud could have experienced more than one incident.

3: Types of fraud

This chapter identifies and explains the various types of fraud and assesses the involvement of organised crime networks in Queensland. The different types of fraud have been grouped into four different areas; however, many kinds of fraud are interrelated.

The different types of fraud covered in this chapter are those that are considered a current problem. For the purpose of this paper, the various kinds of fraud are grouped into the following four areas:

- internet and online fraud
- credit card fraud and skimming
- identity fraud
- cheque fraud.

The internet and online fraud

Background

In the last decade, internet use has significantly increased as a means of communicating, accessing information and undertaking commerce. The internet provides many benefits for users, including convenience, speed, accessibility and cost-effectiveness (Krone & Johnson 2007). Between 2001 and 2008, internet usage by Australian consumers more than doubled, from 35 per cent of the population (ABS 2006) to 74 per cent (Internet World Stats).

More and more people are using the internet for banking and paying bills as banks reduce the number of branches and the need for face-to-face contact with bank employees. Consumers are now able to apply online for home, car and personal loans, credit cards and home and contents insurance (Barker 2002). According to the Australian Computer Emergency Response Team (AusCERT) Home Users Computer Security Survey, 84 per cent of participants used their computer for internet banking (AusCERT 2008).[5] The United Kingdom's Association for Payment Clearing Services (APACS) identified that between 2001 and 2006 the greatest proportion of new internet banking users were persons in the over-55 age group (APACS 2007).

With the creation of tools to capture sensitive personal information, offenders need no longer trick or deceive internet users into providing their details. The creation of malicious software (malware) enables criminals to obtain personal information, often without the computer user's knowledge (see p. 9 for more details).

5 This was from a sample of 1001 people.

According to internet security company McAfee (2006, p. 2), 'cybercrime represents the fastest-growing category of crime globally'. Traditional law enforcement methodology alone cannot be relied on to investigate computer crime. There is a need to build relationships and partnerships with private companies, financial institutions and government agencies, both nationally and internationally, to assist in combating online fraud.

Risks of the internet

With advances in technology and an increase in electronic storage, transmission and sharing of data, online crimes have become easier to commit and harder to track (ABS 2008; Walters & Galvin 2008). Increased internet usage by Australians has led to a heightened exposure to online fraud. Individuals and organisations have become increasingly reliant on computers to store, communicate and process information, which has led to an opportunity for the technologies to be misused (Urbas & Choo 2008). According to the 2008 AusCERT Home Users Computer Security Survey (p. 28), more people felt 'comfortable' (40%) providing personal information online than those who felt 'uncomfortable' (8%) or 'very uncomfortable' (5%).[6] The United Kingdom's Serious Organised Crime Agency (SOCA) in its 2008 threat assessment found that the ease of obtaining personal information online was the greatest enabler to fraud offenders and that attempts to do this were increasing.

Many users of the internet have only a basic knowledge of its operation and lack security knowledge. This allows users' computers to be easily compromised by fraud offenders. It has been suggested that it may take from only four to thirty minutes for an unprotected computer with an internet connection to be compromised by malicious software (Bradley 2003; Choo 2007; Loney 2004; Sophos, cited in LeMay 2005).[7] As noted by AusCERT, the home computer was never designed for secure financial transactions (Hodge 2005).

One of the drawcards for fraud offenders using the internet is the anonymity it affords them. Advances in information and communication technology have made it easier for fraud offenders to mask their identity through the use of anonymous email accounts, security tools, using another person's computer login and proxy servers (Smith 2007b; SOCA 2008). Remaining anonymous enables fraud offenders to minimise, and in most instances avoid, detection and law enforcement attention. The internet has also meant that there

6 Sample of 1001 people.

7 'Unprotected' means a computer without anti-virus, anti-malware and firewall protection.

is no face-to-face contact between the fraud offender and the victim. The anonymity provided by the internet to fraud offenders results in a low risk of detection for a relatively high return. This combination makes the internet an attractive option for some organised criminal networks when compared with traditional offences such as armed robberies and drug distribution.

The internet is a global entity without borders. This raises jurisdictional questions and makes the prosecution of offenders complex and difficult. The global nature of the internet also allows criminal networks to expand internationally and communicate without being highly visible to law enforcement (SOCA 2008).

The internet is low cost, readily available and accessed by millions of people globally. Fraud offenders require only 'some knowledge, a computer and an internet connection' to commit a variety of fraud online (Kaspersky, cited in Dearne 2009, p. 26). The introduction of black-market web portals, discussed later in this paper, has helped to give fraud offenders the relevant information to perpetrate all kinds of fraud. Wahlert (1998) has described the internet as a 'big laboratory' where fraud offenders can share the tricks of the trade, hone their skills and develop tools.

With the increase in portable devices that are able to connect to the internet, such as mobile phones, wireless laptops and palm pilots, new forms of exploitation are occurring because security systems are low-level or non-existent (Urbas & Choo 2008; Choo 2008). It has been suggested that one in three mobile phone owners use their mobile phone to connect to the internet, and that an estimated 800 million people worldwide will access social networking sites on their mobile phone by 2012, compared with only 82 million in 2007 (Fenech 2009). Furthermore, as telecommunication companies expand their networks, thereby increasing bandwidth, there will be an increase in the number of fraud offenders and victims taking advantage of wireless technologies (Choo 2008).

Methodologies employed by criminals are evolving to include information technology (IT) skills and knowledge because of an increased dependence on IT throughout the general population. The skills used by online fraud offenders will undoubtedly increase in the future, because technical developments are occurring at such a rapid rate that law enforcement agencies will need to continually improve and monitor their responses.

Malicious software (malware)

Malicious software (malware) is a term for computer code that is secretly installed on a person's computer. Malware can infect computers by means of:

- an email with the virus attached
- an email with a link in the body of the email that when clicked activates the malware
- a victim visiting a compromised website (as in case example 1 below).

Malware allows information contained on the computer to be sent back to a third party. The computer can then be remotely accessed and used in conjunction with other systems to cause serious harm (Australian Communications and Media Authority 2007; OECD 2008).

CASE EXAMPLE 1

Commonwealth Bank online banking website compromised

In late 2007, customers of the Commonwealth Bank of Australia (CBA) were targeted by a Trojan virus. When customers went to the correct and secure banking site, a Trojan inserted an extra box on the webpage which captured a special password reserved for transferring funds overseas. When the customer transferred money, the Trojan created an additional transaction which was sent to a money mule's account (Walters & Galvin 2008).

About one in six Australian home computers are compromised by malware (Walters 2008a) and in 2008 Australia was the sixth most targeted country in the world for Trojan attacks (Chia Fei, cited in Walters & Galvin 2008).

Given the difficulties of online detection, the degree to which Queensland-based organised criminal networks are involved in installing malware on computer systems is currently unknown. There is no doubt that Queenslanders, and many other Australians, are targeted by these attacks.

Black-market web portals

Black-market web portals (BMWPs) are online forums where criminals are able to:

- share information
- trade in stolen data
- learn how to commit online offences
- conduct training modules
- discuss new methodologies and vulnerabilities
- trade viruses, mailing lists and spamming tools
- trade personal financial and identity information.

BMWPs provide a forum in which data can be easily trafficked, and this, according to Dearne (2008, p. 27), is 'emerging as a major organised crime activity worldwide'. Case example 2 shows the cost of buying fraudulent bank cards, as listed on one BMWP.

It is not known how many BMWPs exist, but as soon as law enforcement shuts one down it is likely that others take its place. Typically, transactions conducted through BMWPs rely

on payment using Western Union (Walters 2008b) and International Moneygram. This further removes fraud offenders from the risk of being identified.

Because of their anonymous nature and the ease with which information can be shared, it is likely that BMWPs will continue to flourish and be relied on by criminals.

CASE EXAMPLE 2

The use of BMWPs to purchase fraudulent credit cards

According to one BMWP site, people can purchase blank plastic cards for $35 to $45 each, depending on the quantity. Cards embossed with account numbers can be bought for $70 to $80 each, depending on the quantity, and if fraud offenders require cards with holograms, the additional cost is around $5 each for a minimum purchase of 500 cards.

Phishing

Phishing is an attempt to obtain a person's personal details such as account numbers, passwords and credit card details. Fraud offenders are able to download from the internet phishing kits that provide a convincing copy of a legitimate financial services website (Galvin 2008). Phishing can be carried out in a number of ways, including by email, by phone, by post and in person. The request is usually from someone purporting to be from a business or financial institution. Often, an email containing a phishing request will simply ask for personal details to be emailed back or it will direct the person to a hoax website where they are asked to verify their account details (ABS 2008). Once obtained, these details can be used by fraud offenders to commit identity fraud offences and credit card fraud.

According to Walters (2008a), consumers are now more aware of phishing attacks, so fraud offenders are finding that the technique has lost much of its effectiveness. In 2007, only 0.4 per cent of people fell victim to phishing scams.[8] According to security company McAfee, fraud offenders are moving away from the typical 'update your banking details' emails to more varied and directed messages. Some phishing attacks have been targeting online auction houses, using emails that appear to have been sent by another user. For example, the emails may claim that the sender has raised a dispute against you, ask you questions about an item, or state that you have not paid for an item you purchased (McAfee 2006).

As people become ever more reliant on mobile phones with an internet connection, phishing via text messages ('SMiShing') may increasingly be used by fraud offenders intent on infecting the mobile phone with malware or viruses (McAfee 2006). In a recent scheme identified by an anti-virus company as circulating in Russia, India and Indonesia, a virus can command a phone to text premium services set up by the fraud offender and charge 40 to 90 cents a time. It takes just one infected mobile to contact another and the virus spreads. Security software developer Kaspersky Labs suspects that Australia will be targeted and Australian software companies are expected to release anti-virus protection for mobile phones late in 2009 (Sun 2009).

Individuals and organised fraud networks around the world who are involved in phishing scams are not limited by state or country boundaries. If the fraud offenders wish to sell the information they have obtained, they need access to a network. By operating globally, the fraud offenders are able to target more people and are able to sell their product more easily. The extent to which organised criminal groups are involved in phishing scams is difficult to determine, but it is not likely that the organised networks who are committing these scams are operating from within Queensland.

Advance fee fraud

The concept behind advance fee fraud (AFF) or Nigerian '419' scams[9] is to persuade victims to send an amount of money by making them believe that by doing this they will eventually receive a lot more. Australians are continuing to fall victim to AFFs and are losing millions each year as a result. African countries have typically been associated with AFFs; however, countries such as Spain, Italy, Russia and Romania are emerging as major initiators of these scams.

The effects of AFF on Queensland have been such that the QPS has introduced several initiatives in a bid to reduce the number of victims and the amount of money lost to these scams:

- Operation Echo Track (2006) commenced to 'disrupt and monitor fraudulent funds being transferred to Nigeria' (QPS 2008a, p. 18).
- Project Synergy was created to 'increase public awareness and build capacity of Queensland government agencies and industry groups to work together in partnership to combat fraud through best practice' (QPS 2008a, p. 19).
- A website was launched for victims of AFF scams to report directly to the country to which they have sent money (QPS 2008b, and Waters 2009, p. 32).

Members of the community facing financial struggles as a result of the current global financial crisis may be more susceptible to 'get rich quick' schemes. People who may not otherwise have been taken in by AFFs can become victims when they are under financial pressure.

8 This equates to 57 800 people who fell victim to phishing attacks in 2007, according to the ABS (2008).

9 The term 'Nigerian "419" scams' refers to s. 419 of Nigeria's Criminal Code, which outlaws the practice.

eBay fraud

Online auction houses are increasingly being used by fraud offenders to scam unsuspecting victims, but the full extent of the activity is unknown. This is in part because victims may not report the scam or they may report directly to the auction house for action. In other instances, when victims report to police over the counter, there is often difficulty determining the complete circumstances of the offence and, as a result, it may not be recorded.

In 2007, the QPS, in partnership with eBay, commenced the eBay Project. This involved setting up a website where victims of eBay fraud from around Australia can report online. The details of the fraud is then forwarded to the relevant law enforcement agencies throughout Australia for investigation. In instances where the offender is located overseas, an Interpol request is compiled.

Scams

The purpose of many scams is to either receive money or to obtain a person's particulars through deceptive means (ABS 2008). There are numerous online scams currently operating around the world and often they are the same scams that have been used for years, only a little more refined. Where once scams were conducted by mail or in person, many are now occurring online, often by email. This is most likely the result of increased internet use by members of the public and the ease of appearing legitimate online and disguising the fraud offender's true intent (Wahlert 1998).

The current global financial crisis may result in more people falling victim to scams. Some people may be so eager to make easy money that they let their guard down and are less likely to question the legitimacy of the external request.

The complexity of the internet makes it difficult to determine the extent to which Queensland-based organised networks might be involved.

Summary

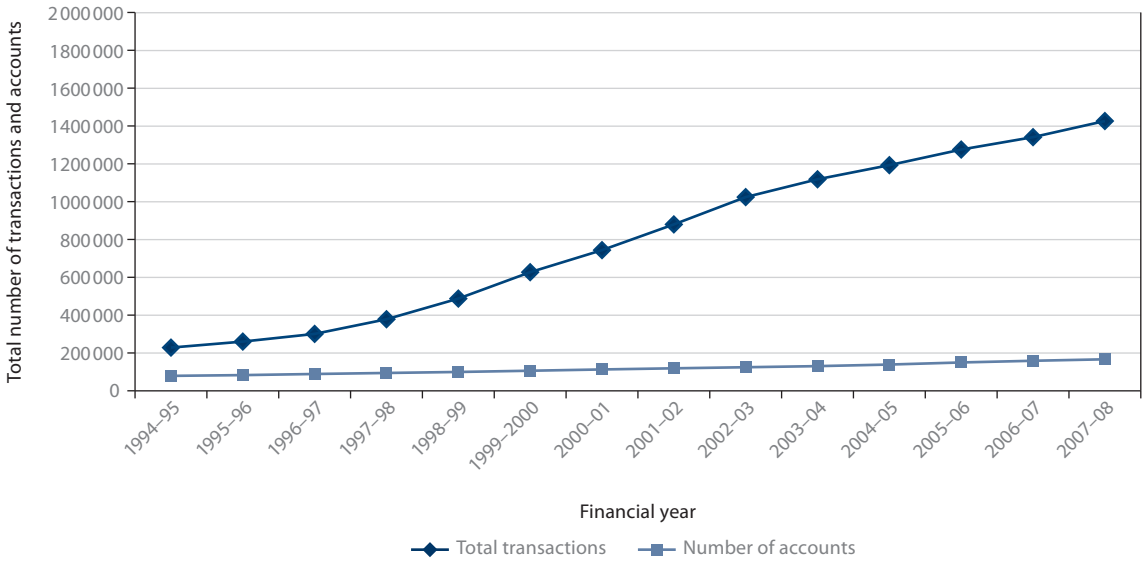
The internet and technology have significantly assisted organised criminal networks to fraudulently obtain personal details and information to use for their benefit. Dependence by the wider population on information techology has meant that the methodologies used by criminals are evolving to include this as part of their offending. Organised criminal networks offend online because the internet provides anonymity, security, a high return for a relatively low risk, and a global network in which to target victims. Sophisticated criminal groups do not appear to be operating from within Queensland. Online fraud is conducted globally by organised networks and the resulting financial and emotional effects on Queenslanders are significant.

Credit card fraud and skimming

Credit card fraud

According to figures released in 2007 by the Australian Payments Clearing Association (APCA), there were 43 million plastic debit and credit cards on issue to Australians as at 2007 — about 2.5 cards for every Australian over 18 years of age. Reserve Bank of Australia (RBA) figures show that, since the financial year 1994–95, the number of credit card accounts has remained relatively stable, whereas the number of transactions conducted on these cards has increased exponentially (see Figure 1). This means that consumers are conducting more transactions with their credit cards,

Figure 1: Credit card transactions and number of credit card accounts in Australia, 1994–95 to 2007–08



Source: Reserve Bank of Australia. Credit and charge card statistics, <www.rba.gov.au/Statistics/Bulletin/C01hist.xls>.

increasing the chances of that information being captured and then used by fraud offenders.

QPS statistics show that credit card fraud has steadily decreased since a peak in the financial year 2002–03. Reported credit card fraud for the financial year 2007–08 are about half what they were in 1998–99 (see Figure 2). There are two possible reasons for this. First, new crime classes have been created on the Queensland Police Records and Information Management Exchange (QPRIME) and offences that may have previously been reported under one crime class are now falling under other classes. Second, it may be that victims are not reporting credit card fraud to law enforcement and the matter is being dealt with directly by their financial institution.

Statistics published in the ABS Personal Fraud Survey (2008) show that, of the 383 300 people who were victims of credit or bank card fraud in the 12 months prior to undertaking the survey, the majority of victims were employed (78%), were born in Australia (70%) and were married (67%); 27 per cent were aged 35 to 44 years and 43 per cent had a highest educational attainment of at least a diploma, a degree or another higher qualification. Interestingly, 29 per cent of victims reported that their most recent incident involved having their card details taken from them in person as opposed to over the internet or by telephone (ABS 2008).

Obtaining a person's credit card details can occur in a number of ways:

- the use of phishing
- malware on a victim's computer
- obtaining discarded carbon imprints of credit cards
- skimming card details or theft of a physical card.

With the decline in cheque use by Australians and the increased use of credit cards, particularly for 'card-not-present' transactions[10] for overseas purchases using the internet and telephone (Australian Bankers Association 2008), it is predicted that this payment method will continue to be exploited by hackers and fraud offenders. The anonymity and the ease of perpetrating online fraud has also helped to make credit card fraud easier to commit. Case example 3 describes how online auction houses were used to dispose of thousands of goods purchased using fraudulent credit cards.

CASE EXAMPLE 3

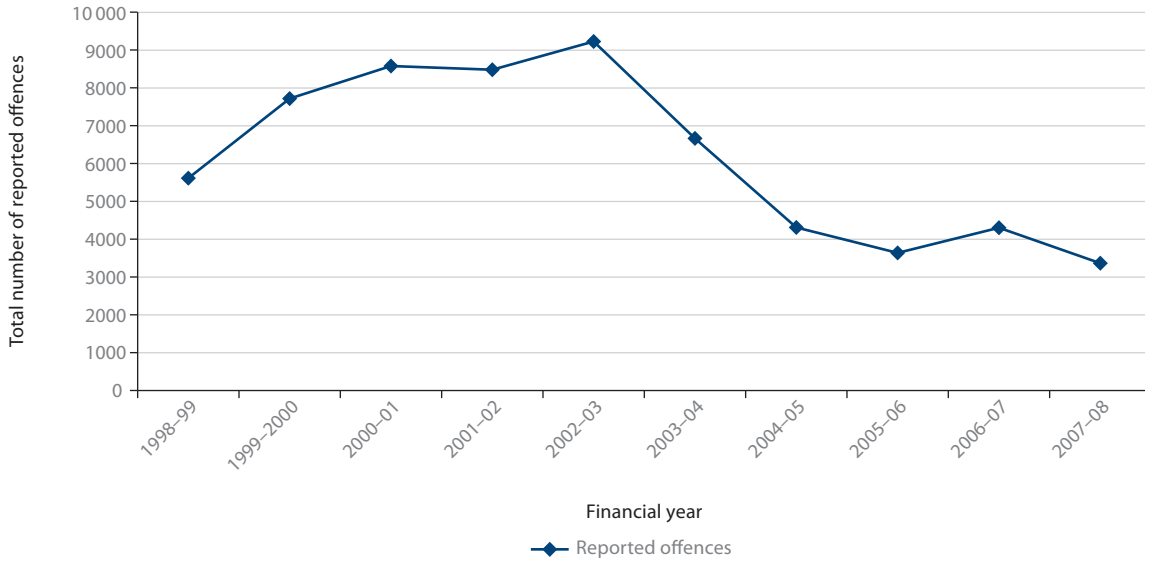
NSW Strike Force Bachelor

In February 2009, Strike Force Bachelor was commenced to investigate the sale of store gift cards being sold at reduced prices through online auction houses. Subsequent investigations identified two men who are alleged to have used stolen credit card numbers to buy more than $4.5 million worth of items, which they then sold on eBay and other online auction houses at significantly reduced prices. As well as the gift cards, items included televisions, computers, cameras, steam cleaners and bottles of expensive wine. The pair operated for approximately two years and in that time sold 6000 items online for $1.3 million (Barrett 2009; NSW Police 2009).

Much of the credit card fraud in Queensland is committed at a lower, more opportunistic level and can involve offences, such as stealing cards from mailboxes or persons, refunding

10 'Card not present' refers to transactions where it is not possible for a physical credit card to be shown. This occurs in transactions over the telephone, on the internet or by mail order.

Figure 2: QPS reported fraud by credit card offences in Queensland, 1998–99 to 2007–08



money back into accounts using electronic funds transfer at point of sale (EFTPOS) terminals, or stealing carbon imprints of credit cards that had been thrown away.

For more serious credit card fraud, there does not appear to be organised criminal groups operating solely within Queensland. Most credit card fraud appears to be run nationally and internationally, often with links to Malaysia. This could in part be because Malaysia has implemented chip technology (discussed in more detail from p.15), making it more difficult for people to copy credit cards in this country. Low-cost flights from Asia and the relative wealth of Australians may be other reasons for this country being targeted. Given the global nature of the internet, fraud offenders are able to operate on an international scale and are not limited to state boundaries, as discussed in case example 4.

CASE EXAMPLE 4

Malaysian cells involved in counterfeit credit cards and false documents

A sophisticated and organised, multi-tiered international criminal syndicate involving Malaysian nationals is operating in Australia. In January 2009, the QPS uncovered several cells who had links interstate and to Malaysia.

One cell, operating on the Gold Coast, had an embossing machine and more than 200 blank credit cards bearing the names of various financial institutions. Another cell operating in Brisbane was located with 42 gift cards (worth about $13 000), 28 counterfeit credit cards and false documents.

All persons involved in the various cells were Malaysian nationals. It is alleged that these cells had the potential to cost banks, retailers and account holders about $1 million (MacDonald 2009a & 2009b; Molloy 2009; O'Brien 2009; Wray 2009).

The numerous ways in which credit card details can be obtained, the affordability of purchasing card details,[11] the anonymity and the ability of criminals to easily enter the market, all make credit card fraud an attractive area for criminal enterprise.

The current global financial crisis may have an effect on credit card fraud in the short term, as people are less inclined to spend and may be more vigilant in checking their bank statements to keep abreast of their spending. Alternatively, fraudulent credit card applications may increase as people struggle financially as a result of the economic downturn.

11 Credit card numbers, including the expiry date and three-digit card verification value (CVV) number, can sell for as little as $2 to $3 each (*Sydney Morning Herald* 2008).

Money mules

Money mules are people who are recruited to receive sums of money into their account and then forward this money to the organisers of the fraud. Often, fraud offenders entice people to work as mules for them by advertising positions such as international sales representatives, financial managers or shipping managers (Crawford 2008). These job advertisements can be placed on employment websites or can be spam advertisements sent by email. (See the appendix at the end of this report for an example of a recruitment email.) Fraud offenders use the brand names of well-known organisations and have been known to create false websites and to set up email addresses linked to them in order to appear legitimate. Mules are asked to send their personal details, including details of bank accounts, to the fraud offender and to await notification that money has arrived in their bank account. The mules are then advised to withdraw the money, retain a commission for their assistance, and forward the remainder of the money using Western Union.

Money muling is an organised criminal activity and exists in Queensland. Often, as in case example 5, money mules are not aware that they are participating in a fraudulent and money laundering scheme with money that has been stolen or unlawfully obtained.

CASE EXAMPLE 5

Russian dating site recruiting Australian money mules

In September 2008, a Queensland account holder at a financial institution identified two unauthorised transactions from her account, totalling more than $16 500. These transactions had been credited to another account within the same institution. The owner of the second account, who resided in New South Wales, had unknowingly been used as a money mule.

The money mule had met a 'female' on an online dating site. In an email to the mule, the 'female' nominated two financial institutions and asked the mule to open an account at either one. The 'female' told the mule that 'her' sister had accounts at both of the financial institutions and that, if the mule set up an account, money could be transferred more easily between the accounts.

It is unknown how the transfers occurred, but it is believed that a Trojan virus was placed on the victim's computer.

Outcome: The first of the two transfers was withdrawn in cash by the mule and sent to St Petersburg in Russia using Western Union. The second transfer was able to be reversed by the financial institution.

The use of money mules is expected to increase because it provides an easy way for fraud offenders to distance themselves from the offence. With the current global financial crisis, organised fraud offenders are taking

advantage of cash-strapped employment seekers (Crawford 2008). People who may not otherwise have been lured into money muling may now consider it because of the ease with which they can earn money. Furthermore, people desperate for employment are less likely to ask questions about the legitimacy of the employment.

Skimming

Skimming is the act of illegally copying the data contained on the magnetic strip of credit and debit cards. Once the details are obtained, fraud offenders create fraudulent cards on which the data from a victim's magnetic strip are written. The fraudulent cards are then used to obtain funds from victims' bank accounts (SCAMwatch 2008) or to make purchases.

Skimmers are devices ranging from attachments to automatic teller machines (ATMs), which may have keypad overlays that transmit personal identification numbers (PINs) to a nearby laptop, through to attachments on merchant terminals in stores. There was an instance in New South Wales where a subscriber identification module (SIM) card was placed in a merchant terminal and, while a legitimate purchase transaction was occurring, the SIM card enabled the card's strip information to be sent to criminals overseas (Walters 2008c). Case examples 6 to 10 following describe other types of card-skimming modus operandi.

The ease with which people can buy skimmers over the internet is of concern, and organised networks are becoming increasingly sophisticated in concealing the importation of such devices. People interested in buying a skimmer are able to compare the various features of the different ones (Barker, D'Amato & Sheridon 2008). Some skimmers are able to create counterfeit cards where the information stored on a stolen card can be decoded and new information written on the same card (Barker, D'Amato & Sheridon 2008). There is no doubt that card skimming is difficult to detect, track and prevent; it is often not until victims receive their bank statement 30 to 60 days after the fraud has occurred that they become aware of it (Barker, D'Amato & Sheridon 2008).

QPS statistics up until the 2007–08 financial year showed that only a few skimming devices had been located in Queensland.[12] This could have been for a number of reasons:

- the QPS was not advised by financial institutions when skimmers were discovered attached to their ATMs
- the risks associated with importing a skimmer into Australia and having to install it were a deterrent to potential offenders
- the ease with which credit card dumps could be purchased online, and the low cost of the dumps, made this method of offending a more attractive option than skimmers
- skimmers remained undetected until such time as the victim's card details were used in another location, by which time the device had been removed and was unable to be recovered.

CASE EXAMPLE 6

Skimmer located in Brisbane

In March 2007, a skimmer was found on an ATM in Brisbane. The attachments on the ATM were identical to two found on ATMs in Sydney, also in March. It is believed that an organised network, possibly with overseas links, was involved (Desmond 2007).

CASE EXAMPLE 7

Skimming using telephone lines, Melbourne

In 2004, a Malaysian man was found with 770 credit card numbers. The man had skimmed the credit card numbers over phone lines, using a modem and voice recorder system that is common in Malaysia. He had spent between $200 000 and $300 000 illegally on 81 of the credit cards. The man had links to a fraud syndicate and used a sophisticated device to filter credit card numbers sent by telephone lines in EFTPOS transactions. This technology had not been seen previously by law enforcement. He used a line-tap modem and a voice recorder that deciphered computer signals being transferred through phone lines. They were then decoded to obtain credit card numbers.

The man had been recruited by syndicate leaders in Malaysia and sent to Australia to tap into telephone lines, skim credit card numbers and siphon hundreds of thousands of dollars from shoppers (*Sydney Morning Herald* 2004; Moynihan 2004; Caulfield 2005).

Outcome: The man pleaded guilty to one charge of conspiring to cheat and defraud and was sentenced to three years in jail.

CASE EXAMPLE 8

Importation of skimming device and blank cards

In November 2005, the then Australian Customs Service in Sydney prevented an alleged attempt to import material designed to skim credit cards. Customs officers searched the bags of three Chinese nationals when they arrived in Sydney on a flight from Bangkok. Officers found a skimming device, high-quality blank credit cards and software believed to be used to create counterfeit cards (Australian Customs Service & Australian Federal Police 2005).

12 QPS statistics have not been consulted for the financial year 2008–09.

CASE EXAMPLE 9

Sophisticated card-skimming ring, Sydney

In 2005, a sophisticated card-skimming ring stole more than $1.6 million from 600 New South Wales bank customers. Four foreign nationals on student visas (linked to Canada and Bulgaria) fitted ATMs with electronic card readers hidden behind a false front, with a tiny videocamera hidden behind opaque plastic to capture PINs. The men would often watch the ATM from a nearby café and, after several hours, would detach the device, transfer the details onto fake cards and match the account details with the PIN (Dearne 2005).

These men were not the organisers but had been picked because of their financial problems.

Outcome: The four men were jailed for terms between 16 months and 22 months (Jacobsen 2007).

CASE EXAMPLE 10

Fraudulent credit card activity, Gold Coast and London

In November 2006, an English tourist on the Gold Coast was located by police with $117 944 in cash, a laptop containing the details of 1800 stolen numbers and PINs from valid credit and debit cards, a credit card reader/writer and a large number of telephone cards with magnetic strips. The man had encoded the stolen credit and debit card details onto the telephone cards and used them to withdraw cash from ATMs. The card numbers had allegedly been obtained from a relative who ran a number of retail outlets in London (QPS 2008c, p. 16).

Recent media reports suggest that skimmers are being found in increasing numbers. This may be as a result of increased public awareness and educational campaigns aimed at informing the public about what skimmers look like. This could be taken further by placing pictures of skimmers *in situ* on the websites of financial institutions, which might help the public to recognise the different components of a skimmer, and alert potential victims.

Systems to combat/reduce card skimming

There are technologies that can be used to reduce the instances of card skimming, such as chip and PIN technology on credit cards and 'jitters' on ATMs. Australia has begun to implement these technologies.

Smart cards/chip and PIN technology

Magnetic strips on credit cards are now being replaced by smart cards with encrypted microchips. The microchips are able to store data and, unlike cards with magnetic strips, provide enhanced security. Smart cards also require that a PIN be entered for all transactions, further reducing the number of cards able to be used fraudulently. The main impetus for the inception of smart cards was the need to combat card fraud (APCA 2007). It is believed that smart cards are virtually impossible to copy, as the chip interacts in a specific way with a bank terminal. The opportunity for a fraud offender to use a counterfeit card in this manner is almost non-existent (Salek 2008).

Chip and PIN technology is in use in about 45 countries (APCA 2007), including Canada and countries throughout Europe, the United Kingdom and Asia (Barker, D'Amato & Sheridon 2008; Salek 2008). Malaysia introduced microchip cards in 2005 and as at September of that year had virtually no counterfeit fraud (Barker, D'Amato & Sheridon 2008). Australian financial institutions have begun to introduce chip technology and deploy terminals that are able to read the chips. However, as Tung (2008) comments, there has been no real pressure on Australian banks to introduce chip technology as any fraudulent transactions occurring on a customer's card are not borne by the customer. It is easier and more cost-effective for financial institutions to absorb the debt than to introduce chip and PIN technology and bear the costs associated with deploying new terminals.

According to a statement released in December 2008, Visa plans to have several initiatives in place within the next five years. Such initiatives include:

- 100 per cent chip card issuance
- all merchant terminals and ATMs in Australia being capable of reading chip cards
- the requirement of all online merchants to check the three-digit security card code
- enrolling all card holders in Visa's online authentication system, Verified by Visa (Visa 2008).

Although the security features of the smart card may reduce card skimming in the short term, it is likely that in time — as happened when the technology was developed to read magnetic strips — new technologies will be created by fraud offenders that will be able to read, replicate and possibly recode original smart cards. The Serious Organised Crime Agency in the United Kingdom has observed that organised criminals have been able to modify some early models of PIN entry devices (PED) used at some retail outlets so that card information is able to be recorded. Cameras or keylogging software can then be relied on to capture PIN data (SOCA 2008).

Smart cards do not provide any additional security for 'card-not-present' transactions.[13] This means that, if a fraud offender were to get hold of a person's credit card details (because of malware on the person's system, for example), fraud offenders could use the card details to conduct further 'card-not-present' transactions or alternatively write the data onto a fraudulent card's magnetic strip and use the card in countries where chip and PIN technology had not been implemented. SOCA's 2006 threat assessment identified that, as a result of chip technology, fraud committed through 'card-not-present' transactions had increased significantly, particularly in relation to telephone transactions. SOCA also noted that chip technology in the United Kingdom had led to an increase in attempted cheque and mortgage fraud (SOCA 2006).

ATM 'jitters'

Several financial institutions in Queensland have begun to use 'jitters' on ATM card slots. When a bank card is inserted into the machine, the card is 'jittered' (shaken), preventing skimming devices that may be attached from reading the magnetic strip upon entry and exit from the machine. These devices are also able to detect if something is keeping the shutter open (NCR 2008).

Identity theft and fraud

Identity *theft* is 'the theft of a pre-existing identity' (ACPR 2006, p. 10). Identity *fraud* is 'the gaining of money, goods, services or other benefits through the use of a false identity' (ACPR 2006, p. 9). For the purpose of this paper, the term 'identity fraud' is used to cover any form of fraudulent activity involving an identity that is not that of the fraud offender.

Identity fraud is the fastest-growing crime in Australia and has been estimated to cost Australians up to $4 billion annually (Deery 2008). Much of this cost results from poor protection of personal details by members of the community.

Ways in which fraud offenders can obtain a victim's personal information include:

- a victim losing their wallet
- theft of mail
- details provided over the phone or internet
- theft of details from a business's computer system
- online methods such as phishing or malware.

Once obtained, this information can allow somebody to use the victim's credit card details, open bank accounts or take over the victim's entire identity (Australian Institute of Criminology, cited in *Age* 2006). Identity fraud often facilitates other offences, as seen in case example 11.

CASE EXAMPLE 11

NSW Strike Force Gamut

This was an investigation into an organised crime group involved in a multi-million-dollar scam. The group were stealing cheques and personal banking details from mailboxes and using these details to produce high-quality counterfeit documents, including driver licences and Medicare cards. The group used these fraudulent documents to open bank accounts to launder money, which they sent overseas (Gibson 2008, p. 3).

The public rely on personal information to identify themselves for activities such as connecting electricity and telephones and opening bank accounts. If this identity is taken from them, extensive measures are needed for them to prove that they are the person in question. The amendment to s. 408D[14] of the *Criminal Code Act 1899* in 2007 allows for the issuing of a certificate[15] that can be used as proof that a victim has had their identity misused. This certificate is issued by the court after the accused is sentenced on a guilty plea or after an appeal. The certificate records details of the conviction, facts relating to the offence, the victim's details and any other information considered relevant. The certificate does not compel restorative action and is aimed at helping victims of identity fraud to prove — by way of a court decision — that their identity was taken from them. The provision of the certificate goes some way towards acknowledging the difficulties faced by victims in having to prove their identity. A similar arrangement exists in South Australia, and Victoria has recently passed legislation to this effect.

The *Personal fraud survey* (ABS 2008) found that, in the 12 months prior to the survey, there were nearly half a million (499 500) victims of identity fraud. Persons most likely to fall victim to identity fraud were males aged 35 to 44 years who were married, who were born overseas, who possessed a degree, diploma or other higher education qualification and who were earning $2500 or more per week.

Advances in technology have made it easier for criminal groups to obtain personal information and to create legitimate-looking fraudulent documents. Improvements in the quality of scanning equipment, photocopiers, printers and digital image manipulation software have assisted with this

13 Visa has introduced *Verified by Visa* to help customers with online security. Customers are required to create a password attached to their card and, when they shop online at participating online stores, their card is recognised. Once recognised, they are sent a personal message confirming that they are shopping at a legitimate merchant.

14 Section 408D was amended under the Criminal Code and Civil Liability Amendment Bill 2007.

15 Form 46 — certificate under s. 408D(3).

(SOCA 2008). Investigations conducted in the United Kingdom found that the majority of 'forgery factories' were operating from small premises and were capable of large-scale production of false documents (SOCA 2008).

Because of the ease with which false documents can be reproduced, the integrity of documents such as birth certificates, driver licences and passports has been reduced (Office of Strategic Crime Assessments 2000).

Systems implemented to reduce identity fraud

Queensland smartcard driver licence

In 2010, the Queensland Government will begin to introduce a smartcard driver licence to replace the existing type, which has been in use for nearly 20 years. Current driver licences are easy to forge and can be copied using relatively unsophisticated equipment. A computer chip to store personal information will be embedded in the new licences. With the introduction of these cards, Queensland Transport will digitally store people's signatures and photographs in an attempt to 'reduce the likelihood of one person holding multiple cards in different names and assist in identifying if people try to obtain licences using fake or stolen identity documents' (Queensland Transport 2008).

The Australian ePassport

In 2005, biometrics were introduced on Australian passports. Biometrics are 'measurable physiological attributes or characteristics that identify an individual' (DCITA 2004, p. 4), such as fingerprints, overall facial appearance, voice or eyes. In Australian passports issued after October 2005, a microchip is embedded which stores a digital photograph as well as the person's particulars (DFAT).

Although biometrics are considered an effective method for security and identification purposes, there are some problems in using them, such as the possibility that people will be forced to provide their biometrics under duress, or that they may attach their biometrics to a stolen identity (Smith 2007b). The use of biometrics also raises the possibility that private information could be misused. For example, according to Smith (2007b), information:

- might be gathered without permission
- might be gathered without defining the purpose for which it is required
- might be used for purposes other than those for which it was originally obtained
- might be shared without permission.

Although the use of biometrics may be costly to implement and maintain, the cost is decreasing (Zoica 2007), which will make it a more viable option in the future.

Implementation of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

The implementation of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth) (AML/CTF Act) has introduced a number of obligations on reporting entities providing certain financial services. With the introduction of 'ongoing customer due diligence' and 'know your customer' obligations, reporting entities are required to monitor and 'know' their customers. Previously, customers were required to show '100 points' of identification when opening accounts. This is no longer enforced under the AML/CTF Act; however, it is believed that many financial institutions will continue to rely on this method. It is hoped that this Act will decrease the number of fraudulently created accounts. The Act may assist in disrupting identity fraud in that mules now have to attend more financial institutions than previously or handlers may have to recruit more mules so that mule transactions do not appear suspicious.

According to the Australian Crime Commission, 'measures to counter identity crime in the banking, finance and insurance sectors are likely to drive organised criminal groups towards increasingly sophisticated identity crime methodologies and opportunities' (ACC 2007, p. 9).

Introduction of security certificate paper

In 2009, Registries of Births, Deaths and Marriages (RBDM) nationally will implement the use of a new security paper for certificate production. The consistent use of this paper across jurisdictions is vital to the National Identity Security Strategy and is key to minimising the risks associated with counterfeit documents. BDM Victoria introduced the paper in February 2009 and Queensland introduced it in July 2009. The certificates have security features designed to make counterfeiting more difficult and enhance the integrity of the documents (Department of Justice and Attorney-General website).

Cheque fraud

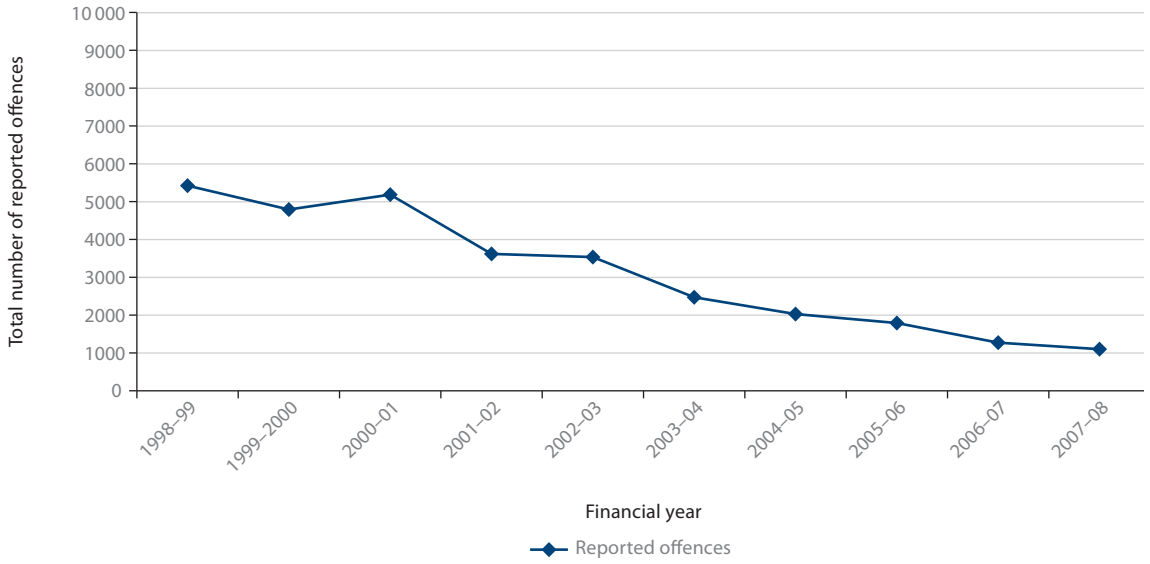
QPS statistics show a decline in cheque fraud (see Figure 3) and this is further confirmed in figures released by the Australian Payments Clearing Association (APCA), which reported that, on an average day in May 2007, 1.8 million cheques were processed; this was 500 000 less than on an average day in May four years earlier. The APCA found that, of the 1.8 million cheques processed, about 10 were fraudulent (APCA 2007).

Although fraud by cheque does still occur, it is mainly conducted by opportunistic offenders who may steal a blank chequebook while conducting a break and enter or hand over a cheque knowing there are insufficient funds in the account. There is no suggestion that organised criminal

networks are involved in the production of counterfeit cheques or the altering of cheques.

As mentioned above, the SOCA believed that attempts at cheque fraud had increased as a result of the introduction of chip and PIN technology. Although there is increased reliance today on cashless plastic transactions, with many of the younger generation having never used cheques, cheque fraud is an area that should be monitored as Australia gets closer to full implementation of chip and PIN cards, given the experience of the United Kingdom.

Figure 3: QPS reported fraud by cheque offences in Queensland, 1998–99 to 2007–08



4: Discussion and conclusions

This chapter assesses the current organised fraud market in Queensland, examines the level of risk to the Queensland community posed by organised fraud networks and outlines proposed strategies aimed at assisting the investigation and reduction of fraud in Queensland.

Assessment of the market

Advances in technology have aided criminals in forging identification documents and bank cards. Improvements in scanning equipment, photocopiers and printers have allowed a much higher quality to be achieved when reproducing these documents and cards. The unsophisticated nature of identification documents has facilitated the ease with which they can be reproduced.

The internet and technology have also significantly assisted organised criminal networks to fraudulently obtain personal details and information to use for their benefit. Dependence by the wider population on information technology (IT) has meant that methodologies used by criminals are evolving to include IT as part of their offending. Online technology has helped organised criminal networks to offend by providing:

- anonymity
- security
- increased knowledge of modus operandi
- a high return for a relatively low risk
- access to a global network in which to target victims
- easy ways of compromising computers
- a lack of borders or jurisdictions.

There do not appear to be sophisticated criminal groups operating from within Queensland conducting online fraud; they operate nationally and globally and their effect on Queensland is significant.

Many fraud offenders rely on black-market web portals to conduct training modules, to discuss new methodologies and vulnerabilities, and to trade viruses, mailing lists, spamming tools and personal financial and identity information. With the vast amount of information contained on black-market web portals, advanced knowledge of how to offend online is no longer required.

Increasingly, people are being recruited by fraud offenders to act as 'money mules' to forward stolen money that has been sent to their bank account. Money muling is an organised criminal activity and is occurring in Queensland. The introduction of various policies under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* may affect money muling activities in that mules may have to attend more financial institutions than previously or handlers may have to recruit more mules.

The current global financial crisis will have an impact on fraud and may make people more susceptible to money-muling activities and more likely to fall victim to scams and advance fee fraud. The economic downturn may also result in reduced spending by consumers on their credit cards and a possible increase in fraudulent credit card applications.

Risk assessment

In the 2004 CMC assessment of crime markets, the risk of fraud being committed by organised criminal networks in Queensland was assessed as MEDIUM–HIGH. The 2004 assessment identified that, although fraud had an organised crime component, most were committed by individuals and loosely associated small groups. Fraud was identified as being an increasing problem.

The 2004 assessment concluded that identity crime posed a HIGH risk. This was the result of a number of factors, such as the ability of identity crime to facilitate many other offences, to undermine the validity of documents and to affect a person's reputation. The assessment concluded that identity crime was increasing.

As identified in this 2009 assessment, the extent of fraud committed by organised criminal networks is limited primarily to online fraud and identity fraud (including credit card fraud). It is deemed that many of the 'street fraud' are committed by opportunistic individuals or groups and not by organised criminal networks. Similarly to the 2004 assessment, this risk assessment analyses the risk of organised criminal groups' involvement in online fraud and identity fraud separately.

RISK ASSESSMENT METHODOLGY
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

Online fraud

- The internet and technology have created an ideal environment for organised criminal groups to enhance their criminality. The internet provides organised criminal networks with anonymity, a huge target base, a high return for relatively low risk, minimal outlays, ease of committing offences and the possibility of making substantial amounts of money — while extensive knowledge of how to offend online is not required. For all these reasons, there is the potential for many traditional offenders to advance to committing offences online, and these offenders have the desire to move into this medium and the confidence to do it. As a result, the *INTENT* has been assessed as **HIGH**.
- The cost of connecting to the internet and obtaining tools to commit offences online is minimal when compared with the potential return. To offend online, organised networks do not require a wealth of knowledge; they can rely on black-market web portals or the recruiting of specialists to provide additional expertise, tools and stolen data, if required. The *CAPABILITY* of organised criminal networks to commit online fraud is assessed as **HIGH**.
- The *THREAT* has been assessed as **HIGH** because intent is HIGH and capability is **HIGH**.
- The harm caused by online fraud to society is varied. There is a widespread perception in the community that online fraud is not as harmful as other offences, and they are often regarded as 'victimless'. Much of this is because of the belief that the banks will carry the cost of such crime. Australians owe close to $45 billion in credit card debt.[16] A percentage of the monthly charges that customers pay goes towards covering the massive fraud bill that is covered by financial institutions. Many credit card holders and bank customers do not realise that financial institutions pass on the costs of fraud in their bank charges. The more money that banks lose to fraud, the harder bank customers will be hit with fees and charges.

  When compared with other types of offenders, fraud offenders receive relatively small punishments, because of the perception that fraud is a victimless crime. Fraud can harm the elderly in particular, as many older people are not able to recover financially because they are no longer in the workforce.

  The potential *HARM* caused by online fraud has been assessed at the **high end of MEDIUM**.
- Consequently, *RISK* is assessed at the **high end of MEDIUM**, as it is a function of threat (HIGH) and harm (high end of MEDIUM). The involvement by organised criminal networks in online fraud is increasing and warrants monitoring.

16 According to Reserve Bank of Australia figures.

Intent	Capability	Threat	Harm	Risk
HIGH	**HIGH**	**HIGH**	**MEDIUM (high end)**	**MEDIUM (high end)**

Identity fraud (including credit card fraud)

- Identity fraud facilitates a broad range of offences, from opening bank accounts in false names through to laundering money by purchasing property or setting up businesses in false names. Much of this is able to occur because of the lack of sophistication of identifying documents and the improvement in quality of printing and scanning equipment. It is well known that there are already many criminal networks involved in the production, supply and use of fraudulent identification, giving other organised groups the confidence to become involved. The desire by organised criminal networks to undertake identity fraud, and their confidence in committing criminal offences using identification that is not their own, results in the *INTENT* being assessed as **HIGH**.
- Technology has greatly increased the ease with which criminals are able to forge identification documents and bank cards. Improvements in scanning equipment, photocopiers and printers have allowed a much higher quality to be achieved when reproducing these documents and cards. The unsophisticated nature of identification documents has made it easy to reproduce them. As a result, criminals are emboldened to use this method as a way of distancing themselves from their criminal activity. The knowledge and resources available to organised criminal networks make them highly capable of relying on false identities to undertake criminal activities. The *CAPABILITY* has therefore been assessed as **HIGH**.
- Since intent has been assessed as HIGH and capability as HIGH, the *THREAT* is **HIGH**.
- It has been reported that identity fraud costs Australia up to $4 billion annually. This is a substantial figure and is significantly higher than for any other crime type. Members of the public rely heavily on identification documents to open bank accounts or to have electricity or telephones connected. When these documents and identities are stolen or tampered with, the harm caused to the victim is significant. Victims often have to go to a great deal of trouble to convince organisations of their identity. The fraudulent copying of documents and bank cards by criminals also harms the integrity of these documents and the ability of people to rely on them. As a result, the *HARM* has been assessed as **HIGH**.
- As the threat has been assessed as HIGH and the harm assessed as HIGH, the *RISK* is **HIGH**. The involvement of organised criminal networks in identity fraud is increasing.

Intent	Capability	Threat	Harm	Risk
HIGH	HIGH	HIGH	HIGH	HIGH

Strategies

Public awareness of computer protection

The QPS and the AFP, through the Australian High Tech Crime Centre (AHTCC), should continue with public awareness campaigns informing the public of the risks of internet use and basic computer security. Law enforcement and other regulatory and government bodies have been working in collaboration to notify the public, particularly through the online medium, of current scams and online fraud targeting Queenslanders. If members of the public are unsure whether they have been targeted, they can easily visit the QPS, SCAMwatch, AHTCC or Office of Fair Trading websites, for example, and obtain information on the different ways in which these types of fraud operate.

The Australasian Consumer Fraud Taskforce[17] has devised National Consumer Fraud Week, aimed at raising community awareness of the dangers of scams and advising people how to protect themselves against scams. In March 2009, National Consumer Fraud Week was set up to coincide with the International Consumer Protection Enforcement Network's Global Consumer Fraud Prevention Month, which involves 30 consumer regulatory agencies from around the world. This initiative provides a way of informing consumers worldwide of the risks of fraud.

Continued fostering of partnerships

Partnerships and relationships with private companies, financial institutions and government agencies need to be fostered, both nationally and internationally, and

17 The Australian Consumer Fraud Taskforce comprises the Attorney-General's Department, the ABS, the Australian Communications and Media Authority, the Australian Consumer and Competition Commission, the Australian Institute of Criminology, the Australian Securities and Investments Commission, the AFP, the Department of Broadband, Communications and Digital Economy, Fair Trading offices from each state and territory, representatives of state and territory police commissioners, the New Zealand Commerce Commission and the New Zealand Ministry of Consumer Affairs.

information-sharing encouraged to assist in combating fraud. Given that much organised fraud is global, the fostering of international partnerships is important. Global cooperation allows information to be shared and law enforcement in other countries to be notified of emerging types of fraud.

Suspension of online banking accounts by financial institutions

Discussions with one financial institution revealed that it is the institution's current practice to suspend customers' online banking access when it is suspected that their computer has been compromised. Where customers have determined that transactions have occurred on their account for which they were not responsible, this financial institution suspends banking access and does not return it until the victim's computer has been cleaned and a receipt issued showing that the computer is free of malware. This financial institution 'wears the cost' of cleaning the computer. The adoption of this procedure by other financial institutions may help to reduce the incidence of customers' accounts being continually compromised.

Creation of a central reporting and strategic body

In 2008, the United Kingdom (UK) introduced a National Fraud Strategic Authority. This agency was established to raise public awareness, identify the key fraud threats in the UK, provide increased support for victims, coordinate and communicate fraud strategies and build the capability to prevent fraud. This agency is made up of stakeholders from both public and private organisations.

In 2009, a National Fraud Reporting Centre will be created to operate in England and Wales, reporting to the National Fraud Strategic Authority. The reporting centre will be a central point of contact for the reporting of cybercrime and will allow the sharing of information and the coordination of investigations. Several other agencies are either in the process of being created or have been created to combat fraud in the UK. They include the National Fraud Intelligence Bureau, the National Cybercrime Unit and the National Lead Force (Heath 2008; National Fraud Strategic Authority 2008).

Depending on the success of the UK model in combating fraud, consideration should be given to the creation of a similar arrangement in Australia.

Presently, there are numerous agencies to which a victim of fraud can report. A central reporting agency would be helpful in determining a more accurate figure for the extent of fraud in Australia, and in identifying trends or patterns. Collecting information through a national central body would assist in determining priorities and the allocation of resources to reduce the amount of information 'slipping through the cracks'. Furthermore, a national body would assist in the creation of strategies aimed at targeting, combating and reducing fraud in Australia.

Conclusion

Organised criminal networks are involved in committing online fraud, credit card fraud and identity fraud; however, there do not appear to be sophisticated criminal groups operating from within Queensland. Organised fraud networks are global in their operation, and the fact that fraud by these groups emanates from outside Queensland's borders does not negate the harm it causes in Queensland.

The nature of fraud in Queensland has changed in various ways since the last assessment in 2004. Different types of online fraud has emerged and become more prominent and widespread, such as malicious software, scams and phishing, and online auction fraud has changed from what was reported in 2004.

The CMC assesses the risk posed by organised criminal networks' involvement in online fraud to be at the high end of MEDIUM and the risk posed by their involvement in identity fraud to be HIGH. The CMC assesses that the involvement of organised networks in online fraud and identity fraud will increase over the next three to five years and it requires monitoring.

Appendix: Example of a money mule job recruitment letter

From: Info
Sent: Wed 10/08/2005 12:55 AM
To: John Smith
Subject: Job Offer

Financial Manager

Velocity Global Resources is a one stop project management agent. It is a virtually managed B2B designed to cater advanced programming services ranging from web application, C++ modules, web designing to data conversion from text to SGML, XML. Our focus is different from the ordinary development companies. We offer exclusively one on one service to corporations, making sure that a whole team is working behind the IT needs of that particular company through their own web based profile, which is secured and will update account information, project status information, bug reports, etc.

We have many ways to save our clients' money. We hire the cheapest programmers and designers all over the world. Our stuff works mostly from home and we don't pay high office rent. That is why our price is the best on the market.

One of these ways to save money is hiring a Financial Manager.
In case of getting order from another country we have to pay 15% fee for international bank transfer according to the US law. To reduce the tranfer cost we are looking for Financial Managers all over the world. When we get an order from another country, the Financial Manager in this country gets the payment and sends it to us through Western Union. Commission rate of Financial Managers is 3%. This way we reduce expences for international bank transfer twice.

In order to qualify for the position, you must be aged 21 and above. The prospective candidate should be good with numbers, committed and a good communicator. No special education is required; however, any experience in accounting / finance / client relations / database management is an advantage. You will be working under the direct supervision of the respective Regional Collections Executive. You receive your commission as soon as the transfer is carried out. There are no probation periods, no rolling reserves and no hidden fees or deductions.

Now required financial manager in:
The United Kingdom
Australia
New Zealand

more info click here

Source: AusCERT, *2006 Australian Computer Crime and Security Survey*, University of Queensland, Brisbane, 2006, p. 28.

References

ABS — *see* Australian Bureau of Statistics.

ACC — *see* Australian Crime Commission.

ACMA — *see* Australian Communications and Media Authority.

ACPR — *see* Australian Centre for Policing Research.

Age 2006, 'Fraud costing Australia 1.1b a year', 7 April 2006, accessed 6 April 2009, <www.theage.com.au/news/National/Fraud-costing-Australia-11b-a-year/2006 04/07/1143916706049.html>.

APACS — *see* Association for Payment Clearing Services.

APCA — *see* Australian Payments Clearing Association.

Association for Payment Clearing Services 2007, 'Online banking usage amongst over 55s up fourfold in five years', press release, 24 August 2007, accessed 22 January 2009, <www.apacs.org.uk/media_centre/press/08_24_07.html>.

AusCERT — *see* Australian Computer Emergency Response Team.

Australian Bankers' Association Inc. 2008, 'Billions of transactions, fraud incidence remains low', media release, 30 May 2008.

Australian Bureau of Statistics 2006, 8146.0.55.001 *Census: patterns of internet access in Australia 2006*, Australian Bureau of Statistics, Canberra, accessed 6 November 2008, <www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0.55.001Main+Features12006?OpenDocument>.

—— 2008, 4528.0 *Personal fraud survey*, Australian Bureau of Statistics, Canberra, accessed 6 November 2008, <www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf>.

Australian Centre for Policing Research 2006, *Standardisation of definitions of identity crime terms: a step towards consistency*, Report Series, no. 145.3, March, accessed 6 April 2009, <www.acpr.gov.au/pdf/acpr145_3.pdf>.

Australian Communications and Media Authority 2007, *Spyware and malicious software*, accessed 6 April 2009, <www.acma.gov.au/WEB/STANDARD/pc=PC_310528>.

Australian Computer Emergency Response Team 2006, *2006 Australian computer crime and security survey*, University of Queensland, Brisbane, accessed 22 January 2009, <www.auscert.org.au/images/ACCSS2006.pdf>.

—— 2008, *Home users computer security survey 2008*, University of Queensland, Brisbane.

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, Parliament House, Canberra.

Australian Customs Service & Australian Federal Police 2005, 'Skimmers red carded', joint media release, 4 November 2005.

Australian Payments Clearing Association 2007, 'Views/reviews: the payments industry in perspective', *Annual review 2007*, accessed 2 April 2009, <www.apca.com.au/AR2007/docs/APCA-AR07_Complete.pdf>.

Barker, G 2002, 'Why five million now prefer a mouse to a person', *Age*, 20 November 2002, accessed 2 April 2009, <www.theage.com.au/articles/2002/11/19/1037697662219.html>.

Barker, K, D'Amato, J & Sheridon, P 2008, 'Credit card fraud: awareness and prevention', *Journal of Financial Crime*, vol. 15, no. 4, pp. 398–410.

Barrett, D 2009, 'Two held on $4.5m eBay con', *Daily Telegraph*, 11 March 2009.

Bradley, T 2003, 'Computer compromised before you can get coffee', accessed 2 April 2009, <http://netsecurity.about.com/b/2004/12/09/computer-compromised-before-you-can-get-coffee.htm>.

Caulfield, C 2005, 'New card tricks lead to jailing', *Herald Sun*, 11 November 2005, accessed 5 November 2008, <www.news.com.au/heraldsun/story/0,21985,17204465-2862,00.html>.

Choo KKR 2007, *Zombies and botnets*, Trends and Issues in Crime and Justice, no. 333, March 2007, Australian Institute of Criminology, Canberra.

—— 2008, 'Organised crime groups in cyberspace: a typology', *Trends in Organized Crime*, vol. 11, no. 3, pp. 270–95.

CMC — *see* Crime and Misconduct Commission.

Crawford, M 2008, 'More cyber crims call Australia home', *Australian Financial Review*, 11 December 2008.

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

DCITA — *see* Department of Communications, Information Technology and the Arts.

Dearne, K 2005, 'Skimmers get $800,000 in spree', *Australian IT*, 27 September 2005, accessed 10 November 2008, <www.australianit.news.com.au/story/0,24897,16731341-15319,00.html>.

—— 2008, 'Online criminals run a market in stolen financial and identity data', *Australian*, 8 July 2008.

—— 2009, 'Crime pays and so does anti-crime software', *Australian*, 27 January 2009.

Deery, S 2008, 'Thieves snare $4b in ID fraud', *Sunday Mail*, 28 September 2008.

Department of Communications, Information Technology and the Arts 2004, 'Biometrics: an Australian Government perspective', Canberra, December, accessed 5 March 2009, <www.dbcde.gov.au/__data/assets/pdf_file/0004/23467/Biometrics_-_An_Australian_Government_perspective.pdf>.

Department of Foreign Affairs and Trade, 'Travel: the Australian ePassport', accessed 5 March 2009, <www.dfat.gov.au/dept/passports/>.

Department of Justice and Attorney-General 2009, accessed 10 July 2009, <www.justice.qld.gov.au/5629.htm>.

Desmond, R 2007, 'Former bank worker spots ATM card skimmer', *Australian*, 22 March 2007, accessed 29 October 2008, <www.theaustralian.news.com.au/story/0,25197,21428067-5006786,00.html>.

DFAT — *see* Department of Foreign Affairs and Trade.

Fenech, S 2009, 'Net surfers gone mobile', *Sunday Mail*, 1 February 2009.

Galvin, N 2008, 'MySpace a new fraud market', *Sydney Morning Herald*, 8 October 2008.

Gibson, J 2008, 'Multimillion ID fraud: man held', *Sydney Morning Herald*, 31 December 2008.

Heath, N 2008, 'National fraud reporting centre to arrive next year', *Law & Policy*, 28 April 2008, accessed 2 March 2009, <http://management.silicon.com/government/0,39024677,39208911,00.htm>.

Hodge, A 2005, 'Home PCs at mercy of bank hackers', *Australian*, 14 March 2005.

Internet World Stats, Usage and Population Statistics, accessed 12 January 2009, <www.internetworldstats.com/>.

Jacobsen, G 2007, 'Four men jailed over $1.6m bank scam', *Sydney Morning Herald*, 19 January 2007, accessed 17 February 2009, <www.smh.com.au/articles/2007/01/18/1169095908954.html>.

KPMG 2006, *Forensic fraud survey 2006*, accessed 6 April 2009, <www.kpmg.com.au/Portals/0/FraudSurvey%2006%20WP(web).pdf>.

Krone, T & Johnson, H 2007, *Internet purchasing: perceptions and experiences of Australian households*, Trends and Issues in Crime and Criminal Justice, no. 330, February 2007, Australian Institute of Criminology, Canberra.

LeMay, R 2005, 'The 12 minute windows heist', 1 July 2005, accessed 2 April 2009, <www.zdnet.com.au/news/security/soa/The12minutewindowsheist/0,130061744,139200021,00.htm>.

Loney, M 2004, 'Study: unpatched PCs compromised in 20 minutes', 17 August 2004, accessed 2 April 2009, <http://news.cnet.com/2100-7349_3-5313402.html>.

MacDonald, A 2009a, 'Credit card fraud hits $2m', *Gold Coast Bulletin*, 10 January 2009.

—— 2009b, 'Credit card scam busted', *Gold Coast Bulletin*, 10 January 2009, accessed 15 January 2009, <www.goldcoast.com.au/article/2009/01/09/37981_gold-coast-news.html>.

McAfee 2006, *Organised crime and the internet*, Virtual Criminology Report, December 2006.

Molloy, S 2009, 'Credit card fraud ring smashed', *Brisbane Times*, 9 January 2009, accessed 15 January 2009, <www.brisbanetimes.com.au/news/queensland/credit-card-fraud-ring-smashed/2009/01/08/1231004180102.html>.

Moynihan, S 2004, 'Credit card scam cost banks $100m', *Age*, 7 December 2004, accessed 5 November 2008, <www.theage.com.au/news/National/Credit-card-scam-cost-banks-100m/2004/12/07>.

National Fraud Strategic Authority 2008, 'UK toughens up on fraudsters with new anti-fraud authority', news release, 1 October 2008, accessed 2 March 2009, <www.attorneygeneral.gov.uk/attachments/National%20Fraud%20Strategic%20Authority%20comes%20into%20being.pdf>.

NCR 2008, accessed 2 April 2009, <www.ncrsecure.com/Documents/NCR_Secure_Brochure.pdf> and <www.ncrsecure.com/Documents/globalfraud.pdf>.

NFSA — *see* National Fraud Strategic Authority.

NSW Police 2009, 'Two charged over multi-million dollar fraud syndicate', media release, 11 March 2009, accessed 16 March 2009, <www.police.nsw.gov.au/news/latest_releases?sq_content_src=+dXJsPWh0dHBzJTNBJTJGJTJGd3d3LmViaXoucG9saWNlLm5zdy5nb3YuYXUlMkZtZWRpYSUyRjU0NDMuaHRtbCZhbGw9MQ==>.

O'Brien J 2009, 'Fruit pickers accused of credit card scam', *Courier-Mail*, 9 January 2009, accessed 12 January 2009, <www.news.com.au/couriermail/story/0,23739,24891059-952,00.html>.

OECD — *see* Organisation for Economic Co-operation and Development.

Office of Strategic Crime Assessments 2000, *The changing nature of fraud in Australia*, Attorney-General's Department, Canberra.

Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, Committee for Information Computer and Communications Policy 2008, 'Scoping Paper on Online Identity Theft', Ministerial Background Report 2007/3/Final, OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17–18 June 2008.

OSCA — *see* Office of Strategic Crime Assessments.

QPS — *see* Queensland Police Service.

Queensland Police Service 2008a, 'Project Synergy takes the sting out of scams', *Police Bulletin*, no. 331, October 2008, pp. 18–19, accessed 1 July 2009, <www.police.qld.gov.au/Resources/Internet/services/reportsPublications/bulletin/331/documents/page%2018_Project%20Synergy.pdf> and <www.police.qld.gov.au/Resources/Internet/services/reportsPublications/bulletin/331/documents/page%2019_Making%20sure%20crime%20does%20not%20pay.pdf>.

—— 2008b, 'Advance Fee Fraud including scams from Nigeria and other West African Nations', Queensland Police Service website, 20 November 2008, accessed 29 January 2009, <www.police.qld.gov.au/programs/crimePrevention/eCrime/scams/Nigerian_Scams.htm>.

—— 2008c, 'Fraud group pins card-skimming tourist', *Police Bulletin*, no. 331, October 2008, p. 17, accessed 1 July 2009, <www.police.qld.gov.au/Resources/Internet/services/reportsPublications/bulletin/331/documents/page%2016_Fraud%20Group%20pins%20card-skimming%20tourist.pdf>.

Queensland Transport 2008, 'New Queensland smartcard driver licence', accessed 6 April 2009, <www.transport.qld.gov.au/Home/Licensing/New_qld_smartcard_driver_licence/>.

Reserve Bank of Australia 2001–2009, accessed 6 April 2009, <www.rba.gov.au/>.

Rollings, K 2008, *Counting the costs of crime in Australia: a 2005 update*, Research and Public Policy Series, no. 91, Australian Institute of Criminology, Canberra.

Salek, N 2008, 'Fighting fraud with chip & PIN', *Secure Computing Magazine*, 27 March 2008, accessed 21 January 2009, <www.securecomputing.net.au/Feature/106597,fighting-fraud-with-chip--pin.aspx>.

SCAMwatch website 2008, Australia Competition and Consumer Commission, Commonwealth of Australia, accessed 6 April 2009, <www.scamwatch.gov.au/content/index.phtml/itemId/693900>.

Serious Organised Crime Agency 2006, *The United Kingdom threat assessment of serious organised crime 2006–2007*, Serious Organised Crime Agency, London.

—— 2008, *The United Kingdom threat assessment of serious organised crime 2008–2009*, Serious Organised Crime Agency, London.

Smith, R 2007a, *Consumer scams in Australia: an overview*, Trends and Issues in Crime and Justice, no. 331, February 2007, Australian Institute of Criminology, Canberra.

—— 2007b, 'Biometric solutions to identity-related cybercrime', in Y Jewkes (ed.), *Crime online*, Willan Publishing, Cullompton, pp. 44–59.

SOCA — *see* Serious Organised Crime Agency.

Sun, M 2009, 'Mobile phone virus SMS.Python.Flocker headed for Australia', *Australian*, 28 January 2009, accessed 2 February 2009, <www.theaustralian.news.com.au/story/0,25197,24975113-12377,00.html>.

Sydney Morning Herald 2004, 'Credit card skimmer up in court', 7 December 2004, accessed 6 April 2009, <www.smh.com.au/news/Breaking/Credit-card-skimmer-up-in-court/2004/12/07/1102182258907.html>.

—— 2008, 'Cyber thieves stealing billions', 9 October 2008.

Tung, L 2008, 'AU$90m card fraud bill too little to force chip and PIN', 10 March 2008, accessed 8 July 2008, <www.zdnet.com.au/news/security/soa/AU-90m-card-fraud-bill-too-little-to-force-chip-and-PIN/0,130061744,339286652,00.htm?feed=pt_australian_payments_clearing_association#talkback>.

Urbas, G & Choo, KKR 2008, *Resource materials on technology-enabled crime*, Technical and Background Paper, no. 28, Australian Institute of Criminology, Canberra, accessed 29 January 2009, <www.aic.gov.au/publications/tbp/tbp028/tbp028.pdf>.

Visa 2008, 'Visa announces five-year agenda to strengthen payment security in Australia', news release, 10 December 2008, Sydney.

Wahlert, G 1998, 'Crime in cyberspace: trends in computer crime in Australia', paper presented to the Internet Crime Conference, Melbourne 16–17 February 1998.

Walters, C 2008a, 'ID theft is just one mouse click away', *Sun Herald*, 7 December 2008.

—— 2008b, 'No names: inside the fake identity racket', *Sydney Morning Herald*, 7 October 2008.

—— 2008c, 'Door opens on game of cat and mouse', *Sydney Morning Herald*, 9 October 2008.

Walters, C & Galvin, N 2008, 'The great credit card swindle', *Sydney Morning Herald*, 7 October 2008.

Waters, G 2009, 'Website tackles net cons', *Sun Herald*, 25 January 2009.

Wray, M 2009, 'State's largest credit card scam busted', *Courier-Mail*, 8 January 2009, accessed 15 January 2009, <www.news.com.au/couriermail/story/0,27574,24889053-3102,00.html>.

Zoica, R 2007, 'Decreasing costs of biometric systems and increasing security concerns — the biometrics market is witnessing high double-digit growth rates across all regions', Global Industry Analysts, accessed 5 March 2009, <www.securitysoftwarezone.com/decreasing-costs-of-biometric-review770-7.html>.

Legislation cited in this assessment

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

Crime and Misconduct Act 2001 (Qld)

Criminal Code Act 1899 (Qld)

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. 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