Queensland Parliamentary Library

Identity Fraud

While there are many definitions and descriptions of identity fraud, the term embraces the creation of a false identity for oneself or the use of the stolen identity of another person (identity theft) to impersonate that other person. The stolen or fictitious identity can then be used in a further criminal act. The ways in which identity fraud are committed can be as basic as sifting through the victim's rubbish bin for their bank account statements and documents containing credit card details. However, the activity is becoming more sophisticated and often involves the use of information technology. Not only are computers more affordable but coming with them are tools that are fraudsters' dreams come true – scanners, imaging equipment, and colour printers.

The resource implications for governments, businesses and law enforcement bodies to develop technology, including security software, to counteract identity fraud are enormous due to the rapidly changing technological environment. Even more challenging is attempting to prosecute interjurisdictional criminal activity given that legislation has limited extra-territorial reach. Some of the possible technological solutions include biometrics (e.g. fingerprints, iris recognition technology), authentication, encryption of transactions and public key infrastructure, sophisticated firewall security and data profiling. However, with these innovations come issues about security and privacy.

Nicolee Dixon

Research Brief No 2005/03

Queensland Parliamentary Library
Research Publications and Resources Section

Ms Karen Sampford, Director (07) 3406 7116
Ms Nicolee Dixon, Senior Parliamentary Research Officer (07) 3406 7409
Ms Renee Giskes, Parliamentary Research Officer (07) 3406 7241

Research Publications are compiled for Members of the Queensland Parliament, for use in parliamentary debates and for related parliamentary purposes. Information in publications is current to the date of publication. Information on legislation, case law or legal policy issues does not constitute legal advice.

Research Publications on Bills reflect the legislation as introduced and should not be considered complete guides to the legislation. To determine whether a Bill has been enacted, or whether amendments have been made to a Bill during consideration in detail, the Queensland Legislation Annotations, prepared by the Office of the Queensland Parliamentary Counsel, or the Bills Update, produced by the Table Office of the Queensland Parliament, should be consulted. Readers should also refer to the relevant Alert Digest of the Scrutiny of Legislation Committee of the Queensland Parliament.

ISSN 1443-7902
ISBN 1 921056 01 0
FEBRUARY 2005

Inquiries should be addressed to:
Director, Research Publications & Resources
Queensland Parliamentary Library
Parliament House
George Street, Brisbane QLD 4000
Ms Karen Sampford. (Tel: 07 3406 7116)
Email: Karen.Sampford@parliament.qld.gov.au

Information about Research Publications can be found on the Internet at:
http://www.parliament.qld.gov.au/Parlib/Publications/publications.htm

CONTENTS

EXECUTIVE SUMMARY

The term '**identity fraud**' embraces the creation of a false identity for oneself or the use of the stolen identity of another person (identity theft) to impersonate that other person. The stolen or fictitious identity can then be used in a further criminal act. These crimes can range from obtaining goods or services to financial fraud, voter registration, terrorism or drug trafficking. The stolen or fictitious identity can also be used to avoid obligations to pay tax, to obtain a government benefit, or to gain access to citizenship or medical services (**pages 1-3**).

A 2003 study commissioned by Australia's national financial intelligence agency, the Australian Transaction Reports and Analysis Centre (AUSTRAC), found that identity fraud costs around $1.1 billion each year to Australia. It is said to be difficult to accurately determine the **extent** of identity fraud because not all individual victims report the theft of identifying information (indeed, many may not be aware that it has even happened or realise its occurrence for some time). Organisational victims, especially government agencies and financial institutions, can be reluctant to advise authorities of incidents because it could be seen as an admission that there is some failure in their systems and security (**pages 3-5**).

The theft of an identity and its misuse can take many forms, ranging from the basic to the extremely sophisticated. The **types** of identity theft include finding identification documentation in garbage bins; card 'skimming'; hacking into computers; stealing and forging identification documents, such as drivers' licences; and 'phishing' (**pages 5-6**).

Some 'real life' examples of identity fraud are provided on **pages 6-9**.

There are many **direct** and **indirect costs** associated with identity fraud. In particular, the impact on individuals can be financially and emotionally devastating (**pages 9-12**).

The experience of identity fraud in **Queensland** is set out in **pages 12-14**, including proposals for a 'smart card' licence to help counter it.

Responses aimed at combating identity fraud can take many forms but it seems to be apparent that a combination of approaches is needed. Those include **legislative** responses (**pages 15-20**), such as that taken in South Australia; government **policies** and **strategies**, such as an online verification service for identification documents to be used by government agencies at all levels (**pages 20-23**); **law enforcement strategies** (**pages 23-25**) and **technological solutions** which might include biometric user authentication and national identity cards (**pages 25-31**). The security and privacy implications of technological measures such as biometrics are examined. Possible responses by **industry** and **government agencies** are considered in **pages 31-34**, and measures that could be adopted by general **workplaces** are also outlined in **pages 34-35**. Tips for **consumers** are set out in **pages 35-37**.

1 WHAT IS IDENTITY FRAUD?

While there are many definitions and descriptions of identity fraud, the term embraces the creation of a false identity for oneself or the use of the stolen identity of another person (identity theft) to impersonate that other person.[1] The terms 'identity fraud' and 'identity theft' tend to be used interchangeably by Australian law enforcement bodies and by commentators.[2] The stolen or fictitious identity can then be used in a further criminal act. These crimes can range from obtaining goods or services to financial fraud, voter registration, terrorism or drug trafficking. In addition to direct financial gain, the stolen or fictitious identity can also be used to avoid obligations to pay tax, to obtain a government benefit, or to gain access to citizenship or medical services.

Perhaps the most horrific example of the way in which identity fraud can be used to facilitate a criminal act is seen in the actions of the terrorists who caused planes to crash into the World Trade Centre in New York on 11 September 2001. Two of the terrorists bribed a legal secretary to complete and notarise false affidavits and residency certifications which they then used to obtain official identification papers from the Government, allowing them to board the planes which they then hijacked. This case was not one of stealing another person's identity but a complete use of fictitious identification documents.[3]

The ways in which identity fraud is committed can be as basic as physical theft of a person's identifying information, such as their bank account statements and documents containing credit card details, through methods as simple as sifting through the victim's rubbish bin ('dumpster diving'). However, the activity is becoming more sophisticated and often involves the use of information technology (IT).

The recent surge in identity fraud has been facilitated by technological advancements and the expanding uptake of IT and the Internet by people from all walks of life. Not only are computers more affordable but coming with them are tools that are fraudsters' dreams come true – scanners, imaging equipment, and colour printers. Computer users can be anyone, including criminals and, even,

---

1 H Pontell, '"Pleased to meet you…won't you guess my name?" identity fraud, cyber-crime and white collar delinquency', *Adelaide Law Review*, 23(2), 2002, pp 305-328, p 306.

2 Australian Centre for Policing Research, 'Standardisation of Definitions of Identity Crime Terms', *Discussion Paper* (prepared for the Police Commissioners' Australasian Identity Crime Working Party and the AUSTRAC POI Steering Committee), May 2004, p 2.

3 H Pontell, pp 305-306.

criminal organisations.[4] Many Australians use the Internet for banking and financial transactions that require the provision of credit card or other account details over the Internet. An increasing number of bank customers and shoppers enjoy the convenience of not having to go to a bank branch or store to conduct business. Many government agencies have websites that allow for online transactions and the exchange of personal information in the provision of government benefits or authorisations such as licences. The potential for data to be stolen from commercial and government websites has been realised all too often when security systems have been breached by persons inside and outside of the agency concerned.[5]

Apart from in South Australia, there is no legislation making it a criminal offence to merely steal or assume another person's identity. It is the use of that identity to perpetrate a mainstream crime that tends to be targeted by legislation and law enforcement authorities.

It has been noted that government agencies must have the means of being able to verify that the person who is registering for benefits or services is who they say they are. Not doing so will make them vulnerable to fraud resulting in a loss of public confidence in the agency's operations. The importance of accurate identification is highlighted when it is realised that in 2000, for example, the Australian Taxation Office (ATO) issued around 500,000 tax file numbers, Centrelink processed 4.4 million new claims or re-grants, and the Department of Foreign Affairs issued 1.4 million passports – all of this activity representing just a minor proportion of proof of identity transactions completed by all Commonwealth, State, Territory and Local Governments.[6]

The resource implications for such agencies and law enforcement bodies to develop technology, including security software, to counteract identity fraud are enormous due to the rapidly changing technological environment. Even more challenging is attempting to prosecute interjurisdictional activity given that legislation has limited extra-territorial reach. How do Australian authorities prosecute a person in Europe who uses the Internet to perpetrate identity fraud affecting an Australian individual or company?

Some of the possible technological solutions include biometrics (e.g. fingerprints, iris recognition technology), authentication, encryption of transactions and public

---

4 C Gill, 'Catch me if you can', *Image & Data Manager*, May/June 2003, pp 42-44, p 44.

5 H Pontell, p 307.

6 G Main & B Robson, Commonwealth Attorney-General's Department, *Scoping Identity Fraud*, September 2001, p 1.

key infrastructure, sophisticated firewall security, and data profiling. However, with these innovations come issues about privacy.

2 INCIDENCE OF IDENTITY FRAUD

While official police statistics are kept on the number of crimes recorded involving 'fraud', there is no single category for 'identity fraud'. Many types of crimes involve some degree of fraud. A 2003 study commissioned by Australia's national financial intelligence agency, the Australian Transaction Reports and Analysis Centre (AUSTRAC), found that identity fraud costs around $1.1 billion each year to Australia.[7] Not all of the cost is direct financial cost, however, with around $626 million being concerned with response activities.

It is said to be difficult to accurately determine the extent of identity fraud because not all individual victims report the theft of identifying information (indeed, many may not be aware that it has even happened for some time). Organisational victims, especially government agencies and financial institutions, can be reluctant to advise authorities of incidents because it could be seen as an admission that there is some failure in their systems and security.[8] If the culprit is an employee, this may add to an unwillingness to 'go public'.

In a global survey of large organisations, over two thirds of the companies which responded reported that they had been victims of corporate fraud with around 85% of it being committed internally by employees, particularly senior managers.[9]

A recent survey by the credit reporting service, Baycorp Advantage, found that, in the 12 months to June 2004, of the 10,538 court judgments on small and medium businesses it examined, there were almost 3,500 cases where a senior director or proprietor had a history of bad credit. There were also instances where a business owner used a false identity to hide their bad credit history in order to apply for credit. Baycorp considered that the checks on commercial customers by finance lenders were too superficial and often failed to involve a check on the credit histories of the principals of the business.[10]

---

7 S Cuganesan and D Lacey, Securities Industry Research Centre of Asia-Pacific (SIRCA), 'Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent', September 2003.

8 H Pontell, p 311.

9 C Gill, p 44.

10 Sarah Jones, 'Bad credit histories concealed by fake IDs', *Courier Mail*, 22 November 2004, p 8.

In a study undertaken by the Australian Institute of Criminology (AIC) and PriceWaterhouse Coopers of 155 serious fraud cases prosecuted in Australia and New Zealand in 1998-1999, misuse of identity was found to exist in 38% of the files examined. 24% involved fictitious identities and 13% concerned stolen identities. In one file, an offender was shown to have used 116 different names or identities. It was noted that the data actually reflected conduct that took place up to 20 years ago when misuse of identity was less common due to a lack of technological means to facilitate it. The most frequent ways of using the fraud proceeds were buying luxury items such as cars. Gambling and personal living expenses were also popular ways of employing ill-gotten gains.[11]

A recent trial conducted by the Westpac Banking Corporation with the New South Wales Registrar of Births, Deaths and Marriages to verify birth certificates found that around 13% of such certificates were not an exact match and had been altered, manufactured, or forged. A birth certificate is an important primary means of establishing an identity and, once obtained, can be used to secure other identity documents.[12] A second trial conducted in Victoria between financial services organisations, VicRoads and the Victorian Office of Births, Deaths and Marriages found that 185 birth certificates did not match the records of the issuing authority.[13]

Australia is not alone in facing the problem. A Federal Trade Commission survey in the United States estimated that, in 2002, the cost of identity fraud to business and financial institutions in that country was $US48 billion with consumers losing $US5 billion. The United Kingdom Cabinet Office considers that the cost of the problem to the UK economy was around £1.3 billion in 2000-2001.[14]

It has also been estimated that 37% of online credit card transactions in the United States involve stolen or forged cards. The online vendor of a transaction relating to a purchase of goods or services will not be able to verify that the card or cardholder is genuine (as neither are actually viewed by the vendor), in which case the card issuing financial institution will usually refuse to transfer the money to the vendor.[15]

---

11 Australian Institute of Criminology and PriceWaterhouse Coopers, *Serious Fraud in Australia and New Zealand*, Research and Public Policy Series No. 48, Canberra, 2003.

12 S Ringin, 'Identity Related Crime – A Rapidly Growing Problem', *Artwork*, Oct/Nov 2002, pp 76-81, p 79.

13 S Cuganesan and D Lacey, p 2.

14 Senator the Hon Christopher Ellison, Minister for Justice and Customs, 'New report reveals identity fraud as a billion-dollar threat', *Media Statement*, 12 November 2003.

15 D Curtis, 'Tackling Internet Fraud', *Banking and Financial Services Technology Supplement*, April/May 2004, pp 66-68, p 66.

3 TYPES AND EXAMPLES OF IDENTITY FRAUD

The theft of an identity and its misuse can take many forms, ranging from the basic to the extremely sophisticated. The following methods have been noted by law enforcement agencies –

- Retrieving documents containing personal and/or identifying information from people's rubbish bins or letter boxes. For example, thieves may look for a bank statement with your details on it.

- 'Shoulder surfing' where thieves observe people at ATMs while they are keying in their PINs or listening in while a person provides their credit card number to the person at the other end of their mobile telephone.

- 'Skimming' of credit cards and ATM cards. Skimming is where credit card data is illicitly captured or copied from the magnetic strip on the back, usually by electronic means. It can occur in places such as restaurants where the customer provides a credit card to a waiter in order to pay the bill and the waiter takes it away from the customer for a short time. It can also take place when a person uses an ATM where an electronic device attached to the machine 'copies' the data from the card and the PIN that is entered is observed via a minute hidden camera.

  Over a single weekend, thieves in Sydney stole over $250,000 using the skimming method. One victim of skimming had his card copied at an ATM and his PIN observed, probably with a pinhole camera. Thieves took around $3,000 out of his account over three days. Visa Australia's Risk Manager, Ian McKindley, told a national forum on bank fraud held in Sydney in November 2002 that skimming was on the increase and had risen by 300% in the previous 12 months. Mr McKindley believes that the solution to skimming is a chip card which is a chip in a credit card that has a range of security features to prevent copying. Detective Superintendent Megan McGowan from the NSW Fraud Squad believes that petrol stations are the easiest target for skimmers because of their high numbers of causal employees and rapid staff turnover where, in most instances, details of new employees are not properly checked. They are also places where customers are generally in a hurry and may not notice that their card has been swiped through two pieces of equipment. Australian law enforcement bodies believe that organised crime syndicates are now focussing on Australia due to a strengthening of penalties in South East Asia in recent years.[16]

---

[16] 'Card security warning issued as fraud levels rise', Transcript, *7.30 Report*, 26 November 2002, http://www.abc.net.au/7.30.

- Fraudsters using increasingly available and more affordable IT software and desktop publishing to manufacture licences and other identity documents.

- Hacking into a financial institution's website to obtain e-banking details of customers and then using those details to purchase goods and services.

- Creating fake bank websites which look convincingly like the websites of well-known banks. Online banking has grown considerably over the last three years with around 7 million Australians now engaging in the practice. A new online fraud is 'phishing' which involves a scammer sending bank customers an email which leads them back to a fake bank website at which point the customer unwittingly types in a username and password. The scammer then has the means to enter the customer's bank account. The head of the joint State and Federal Police High Tech Crime Centre said that there have been several instances of 'phishing' since early 2003 which has affected most major banks in Australia. If money is removed from the unsuspecting customer's account, the bank normally covers the cost of the missing money. The potential impact has led one South African bank to issue 80,000 copies of a major anti-virus package to its online customers and some Australian banks are, apparently, planning similar measures. Unfortunately, 'phishing' and other online scams are compromising the uptake of e-commerce in Australia and the popularity of Internet banking.[17]

3.1 SOME 'REAL LIFE' EXAMPLES

Only days after the lists of the missing in the World Trade Centre appeared in the aftermath of the 11 September 2001 terrorist attacks, hundreds of millions of dollars of goods and services were illegally obtained by persons adopting the identities of the victims of the destroyed buildings. The fraudsters went to government agencies claiming that they had lost identifying documents in the WTC collapse and, probably due to the sympathy and grief that was paramount at the time, were able to obtain all sorts of 'new' identity documents such as drivers' licences with very flimsy identifying documentation. Upon getting a driver's licence they were able to obtain credit cards with which to purchase expensive goods and services.[18]

---

[17] 'Online bank customers face 'phishing' fraud', Transcript, *7.30 Report*, 5 May 2004, http://www.abc.net.au/7.30.

[18] C Gill, p 42.

There have been an increasing number of examples of identity fraud in Australia over recent years.[19]

From August 1995 until March 1996, an offender in Victoria used his desk-top publishing equipment to create 41 birth certificates, 41 student identification cards (some with photographs) and a counterfeit driver's licence. He had created these documents on his home computer, scanner and laser printer; giving him the "100 points" of identification required by financial institutions to open an account (see below). Those false documents were used to open 42 separate bank accounts throughout Melbourne. He wrote false cheques and withdrew money from ATMs. He also used these documents to register a business name, obtain sales tax refunds and procure goods from retailers. When caught, the offender was convicted, sentenced to five years' imprisonment and ordered to pay compensation and reparation to the Commonwealth.

A Victorian man used the birth certificates of four babies who died during the 1970s to claim $20,857 in unemployment benefits in the names on the certificates.[20]

A group of car thieves used stolen identities in a complicated car stealing operation. The thieves obtained personal details of people who owned cars of the same make and model as those they were stealing. They then used the stolen personal information to obtain duplicate registration certificates, labels and plates that were then used to re-identify the stolen vehicles. The cars were then sold in another jurisdiction to innocent buyers. Many of the victims whose identities were stolen experienced ongoing problems in trying to show they were in no way involved in the racket. One victim had even had his name changed by deed poll by one offender in order to perpetrate further identity fraud and only found out when he began receiving documents in his new name on a regular basis.

Identity fraud is often committed by a group of people and criminal organisations have been known to deal in the provision of false identity documents, particularly to help people to migrate to other countries and avoid official immigration channels. For example, one syndicate in Australia charged around $100,000 to create new identities for prospective immigrants which allowed the immigrants to

---

[19] Most of the examples that are discussed are, unless otherwise indicated, taken from RG Smith, Australian Institute of Criminology, 'Addressing Identity-related Fraud', *Cards Australia*, Melbourne Convention Centre, 3 September 2003; RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', Paper presented to the Marcus Evans Conferences, *Corporate Fraud Strategy: Assessing the Emergence of Identity Fraud*, Sydney, 25-26 July 2002.

[20] Lou Robson, 'Is this the only way to protect your identity? – Fraud spree costing the community $1.1 billion a year', *Sunday Mail*, 31 October 2004, p 47.

fly into Australia using false documents and begin a new life under new names. Another person left the country on the same documents so that there was no record of the person who came to Australia still being in Australia.

There have been several instances of fraud being committed from within a government or business organisation. For example, a former Centrelink employee used his computer logon identification in a way that caused Electronic Benefit Transfer cards to be issued by the Centrelink computer system in the name of certain pensioners, unbeknownst to those pensioners. The cards purported to entitle the pensioners to credits of various amounts. The former employee used ATMs to withdraw cash of over $20,000 in total. The former employee was sent to prison for over three years and had to pay back the amount stolen to the Commonwealth.[21] In September 2001, a financial consultant, formerly contracted to the Department of Finance and Administration, was convicted of defrauding the Commonwealth of $8.7 million. He did this by accessing the Department's network using another person's name and password. He used other employees' logon codes and passwords to obscure an audit trail and then electronically transferred funds to private companies in which he held an interest.

In July 2004, a wallet found in a Sydney street was handed in to police and in it were computer disks containing templates used to make Medicare cards, drivers' licences, bills from electricity and water companies, bank statements and birth and marriage certificates, all of which could have been used to open bank accounts or obtain other documents. The police found almost faultless NSW, Victorian and Queensland drivers' licences, NSW birth certificates, tax assessment notices, Medicare cards, Australian passport serial numbers, *etcetera*. Interestingly there were also certificates purported to have been issued by the Civil Aviation Authority stating that the holders were fit to fly aircraft! The find of the wallet led to a raid of Sydney premises and the arrest of two men who were charged with 234 forgery related offences. One of the premises, a home of one of the men, contained devices for manufacturing forged documents including a laminating machine, computer, printer and cutting board. Completed and uncompleted forged documents were also found containing names of people the police must attempt to establish exist.[22]

Even a simple electricity bill discarded by a householder would enable a fraudster to make a good profile of the householder, according to Detective Senior Sergeant Darren Stoppa of the Queensland Police Service's Brisbane Identity Crime Unit. If your wallet is stolen, the thief could use a high technology computer and printer to

---

21 RG Smith, AIC, 'Addressing Identity-related Fraud', p 4.

22 Les Kennedy, 'Lost wallet helps unmask identity forging scam', *Sydney Morning Herald* online, 5 November 2004.

change your driver's licence and also produce birth certificates using templates off the Internet.[23]

Fortunately, it appears that Australian identity fraud has not yet assumed the same proportions of the tasteless and bizarre cases noted in the United States where, in one particular instance, a man allegedly murdered a homeless person so he could fake his own death and avoid prosecution for crimes he had committed. In another case, a hospital worker stole the identities of 393 patients. It is possible, however, that similar incidents will be seen in Australia in the not too distant future.[24]

4 IMPACTS AND CONSEQUENES

While there are economic costs resulting from identity fraud that can be roughly calculated, its impact on its victims, both financially and emotionally, is unquantifiable. Some people who have their identities stolen are arrested for crimes they did not commit and may spend a lot of time and anxious effort clearing their name.

In Australia, there is a lack of statistics on the extent and cost of identity fraud, which hinders the ability of governments, business and the public to respond effectively.[25] The House of Representatives Standing Committee on Economics, Finance and Public Administration *Numbers on the Run Report* in 2000 recommended that the Commonwealth Government work with other Governments and industry to develop national statistics on this issue.[26] Accordingly, an AUSTRAC Steering Committee on Proof of Identity undertook to commission and fund research to develop credible estimates of the costs of identity fraud to Australia in order to assist the development of evidence-based policies and to

---

23 Lou Robson, p 47.

24 Commonwealth Government, National Crime Prevention Program, *Identity Theft – A Kit to prevent and respond to identity theft*, February 2004, p 4, citing J Rusch, 'Sweeping Up After Identity Theft', at http://www.osopinion.com/.

25 Commonwealth of Australia, House of Representatives Standing Committee on Economics, Finance and Public Administration, *Numbers on the Run – Review of the Australian National Audit Office Report No 37 1998-99 on the Management of Tax File Numbers*, August 2000, Canberra, Ch 6 (*Numbers on the Run Report*).

26 *Numbers on the Run Report*, para 6.20.

provide a benchmark to evaluate the impact of policies, legislative reform and other changes.[27]

4.1 DIRECT COSTS

The AIC has recently estimated that fraud, including identity fraud, costs Australia $5.88 billion every year.[28] As noted earlier, the 2003 study commissioned by AUSTRAC found that identity fraud costs Australia around $1.1 billion each year.

As mentioned earlier, however, there is significant lack of consensus about the nature and impact of identity fraud in Australia.

4.2 INDIRECT COSTS

4.2.1 Business and Government

A 2003 Global Economic Crime survey by PriceWaterhouse Coopers recognised that there were five indirect costs of fraud to business, and government: damage to reputation; damage to brand and image; effects on share prices (considered to be the most prevalent cost in the longer-term); impacts on staff morale (considered to be the largest short-term consequence); and effects on business relationships.[29]

If the offender is caught, the costs involved in the business or government agency assisting with a prosecution are considerable. Evidence needs to be gathered and staff have to be given time to provide statements and give evidence in court. Even if the offender is convicted, it is not inevitable that the amounts defrauded from the business or government agency will be recovered. It might still be necessary to bring civil action to recover the money, which creates further cost in terms of legal fees and any additional evidence that needs to be prepared.[30]

---

27 As a result, came an independent university research organisation study: S Cuganesan and D Lacey, Securities Industry Research Centre of Asia-Pacific (SIRCA), *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, September 2003.

28 RG Smith, AIC, 'Addressing Identity-related Fraud', p 7, citing AIC and PriceWaterhouse Coopers, *Serious Fraud in Australia*, and Mayhew P, 'Counting the Costs of Crime in Australia', in *Trends and Issues in Crime and Criminal Justice*, No. 243, AIC, Canberra, 2003.

29 PriceWaterhouse Coopers, *Global Economic Crime Survey 2003*, PriceWaterhouse Coopers and Wilmer, Cutler and Pickering, New York, 2003.

30 RG Smith, AIC, 'Addressing Identity-related Fraud', p 9.

In the common situation where computer systems security has been compromised by the identity fraud, the need for upgrading and replacement of software *etcetera* may create considerable expense and, in addition, cause considerable down time. This has negative financial consequences for the business or government agency concerned.

Damage to reputation may be long-term and difficult to restore. For government agencies, it is not easy to restore the public user's confidence in the agency and any systems that have been breached by an offender, particularly if the source was internal.

4.2.2 Individuals

A July 2003 study in the United States considering the impact of identity theft on victims revealed that nearly 85% of all victims find out about their identity theft case in a negative manner (e.g. being refused employment, being denied a credit card, or receiving bills for items not purchased by them) rather than being informed by a business. While victims are finding out about the problem earlier, it is now taking longer to eliminate the negative information from their credit reports.[31] While it does not appear that a similar analysis has been conducted in Australia, one could probably assume that the statistics are similar to those in the US.

A victim may find they no longer have a good credit rating that they have taken years to build up. A person's credit history is built up on data bases of credit reference organisations such as Baycorp Advantage. When an identity is stolen, so is the credit rating that goes with it. If the thief then obtains credit using the stolen identity this may cause the credit rating to plunge into the negative and ruin the chances of the victim of the identity fraud being able to obtain finance for many years. This can also have considerable emotional impact.

Some victims have had to declare themselves bankrupt because of debts run up in their name by identity thieves. For example, a Caboolture woman was recently declared bankrupt when around $10,000 in rent and other bills were charged to her after someone found her driver's licence which she had mislaid.[32]

Innocent victims of identity fraud have also been arrested for crimes committed by the person who has assumed their identity and this can keep happening for a number of years. A student in Adelaide had her wallet stolen and several months

---

[31] USA, Identity Theft Resource Centre, *Identity Theft: The Aftermath 2003 – A comprehensive study to understand the impact of identity theft on known victims as well as recommendations for reform*, Summer 2003, p 4.

[32] Lou Robson, p 47.

later had her driver's licence cancelled due to unpaid fines she had not incurred and received calls from the police saying that she had been drunk and disorderly and was involved in a stabbing. She was also questioned about possessing cannabis and vehicle tampering. The student also received a phone bill for $4,200 for calls she knew nothing about.[33]

Overseas travellers are particularly at risk. For example, an elderly lady from Queensland lost her passport while holidaying in Europe and had $25,000 in hospital bills charged to her name.[34]

5 QUEENSLAND EXPERIENCE

The Queensland Crime and Misconduct Commission (CMC) notes that identity fraud is the most rapidly growing category of fraud offences both in Australia and internationally. It is a high risk crime due to its ability to facilitate a range of other offences. The CMC also commented that the risk posed by identity crime in Queensland will remain high for the next three years unless significant resources are directed at prevention strategies and investment in more sophisticated systems. Experience so far suggests that identity crime has various levels of sophistication.[35]

The Queensland Police Service (QPS) *Annual Statistical Review 2003-2004*, tabled in the State Parliament on 10 November 2004, indicates that fraud offences on the whole had slightly increased in total numbers over the past year but there was an actual 1% decline in the fraud rate. Computer fraud offences increased by 16% since the previous year. The Queensland Police Commissioner, Bob Atkinson, considered that the increase in computer fraud may reflect that there has been more reporting of fraudulent methods such as 'phishing'. In addition, more people are using the Internet to do their banking and pay bills thereby increasing the opportunity for Internet fraud. Commissioner Atkinson believed that media publicity about offenders capturing users' names and passwords through emailing viruses or false websites has resulted in improved community awareness of the issue and, thus, more offences being detected.[36]

---

33 Lou Robson, p 47.

34 Lou Robson, p 47.

35 Crime and Misconduct Commission Queensland, 'Organised crime markets in Queensland – a strategic assessment', *Crime Bulletin*, No.6, September 2004, p 3.

36 Hon JC Spence MP, 'Queensland Police Annual Statistical Review', *Media Statement*, 10 November 2004; QPS, *Annual Statistical Review 2003-2004*, p 13.

It has been reported that 60 people have been charged with 3,000 identity fraud related charges over the past 12 months.[37]

Since 19 April 2004, Queensland motorists have faced more stringent identification requirements when applying for a driver's licence, renewing a licence (if the existing licence is more than two years out of date) or changing their name on an existing licence. In an effort to protect licence holders from identity fraud through having their licences stolen, motorists will need at least three pieces of original identification for new or replacement licences or to renew a licence that is more than two years out of date. This includes at least one primary identification document, such as a birth certificate, and at least one secondary identification document, such as a credit card or Medicare card. Photocopies are unacceptable. A change of name will require an official marriage or change of name certificate rather than the previously acceptable wedding certificates from churches or celebrants. Special measures apply for young students who have trouble meeting the requirements.

The Hon P Lucas MP, Minister for Transport and Main Roads, said that Queensland was the first state to introduce such guidelines as part of a national framework for consistent drivers' licence requirements across all jurisdictions. In addition, the Minister plans to introduce new digital drivers' licences in 2006 with a computer chip that can store personal information to guard against identity fraud.[38] Privacy advocates have expressed some concern, particularly on the basis that if a thief can misuse the smart card licence, the additional information stored on it will create potential for greater damage. They have also questioned the type of information that will be stored on the card and who will be authorised to access it.[39]

At the Brisbane Exhibition in August 2003, the QPS chose to 'showcase' the issue of identity fraud at the same time as releasing a brochure '*when bad things happen to your good name*'. The police sought to show the public the ease with which criminals can steal a person's name and drain their bank accounts. A stall at the Police Pavilion highlighted a credit card skimming machine.[40]

---

37 Lou Robson, p 47, citing Brisbane Identity Crime Unit Detective Senior Sergeant Darren Stoppa.

38 Hon PT Lucas MP, Minister for Transport and Main Roads, 'Drivers Licences', Ministerial Statement, *Queensland Parliamentary Debates*, 22 April 2004, pp 370-371.

39 Office of the Victorian Privacy Commissioner, *Privacy Aware*, 3(1) Autumn 2004.

40 Queensland Police Force (QPS), 'Criminals are targeting your good name', *Media Release*, 11 August 2003, http://www.police.qld.gov.au/pr/news/media/2003.

The QPS has a useful webpage containing fraud information.[41]

6 RESPONSES

Many commentators agree that criminalisation of identity fraud will not be effective on its own. Most existing laws and policies deal with the issue after the crime has been committed and the damage done. It is essential that the issue is seen as a 'whole of community problem' and that governments work with their bureaucracies and industry to develop strategies, such as authentication and verification of identity processes, to reduce and prevent identity fraud.[42]

A number of issues arise when governments and businesses are determining response strategies. The Director of the AIC, Adam Graycar, identifies a few questions that are currently being faced –[43]

- How should Government agencies identify people when they issue primary identification documents, such as birth certificates or passports, and other documents that are often produced as identification such as drivers' licences? Is it sufficient to rely on documentary evidence or should people be asked to provide some sort of biometric evidence like a fingerprint?

- What should financial institutions do to verify the identification documents produced when a person seeks to open an account? Is the "100 points system" governed by the *Financial Transactions Reports Act 1988* (Cth) and its Regulations sufficiently stringent given the greater opportunity and ability technology offers for counterfeiting and manufacturing passports, birth certificates and drivers' licences?

- Would a national identity document issued by the Commonwealth Government assist in the fight against identity fraud or would it be another thing that could be taken and misused by criminals? Would a 'national identity card' type approach be accepted by the Australian public given the disquiet felt by the proposed introduction of an Australia Card in 1988?

- Should government agencies be able to share information with the private sector and vice-versa in order to verify identification of people and to detect

---

41 At http://www.police.qld.gov.au/pr/program/fraud/whatis.shtml.

42 H Pontell, pp 322-323. See also *Numbers on the Run Report*, Ch 6.

43 Adam Graycar, Director of the Australian Institute of Criminology, 'Identity-related Fraud: Risks and Remedies', Transcript, *Radio National*, 4 August 2002, http://www.abc.net.au.

mismatches? Should law enforcement bodies maintain a database of identities that have been used dishonestly?

- What is the right balance in terms of ensuring the accuracy of identification; business efficiency and cost-effectiveness as well as privacy and personal liberty?

6.1 LEGISLATIVE APPROACHES

South Australia is the only Australian jurisdiction so far to directly make identity fraud itself an offence and provide assistance to its victims. Legislation in other states and territories and at the Commonwealth level tends to be specifically directed, such as prohibiting impersonation of a police officer, or comprise long-standing laws regarding forgery and dishonesty. The *Privacy Acts* of the Commonwealth and other jurisdictions do regulate the collection, storage and use of personal information but it are not actually directed at preventing the theft of that information.

The Commonwealth *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* contains provisions that can apply to identity fraud but does not appear to specifically address the issue or deal with actually stealing the identity of another person.

The *Cybercrime Act 2001* (Cth), which inserted new provisions into the Commonwealth *Criminal Code 1995* (Cth), goes some way to enabling electronically perpetrated identity crimes to be prosecuted. It would allow prosecution of identity fraud procured through the misuse of a computer (e.g. gaining unauthorised access to a person's computer) and modification of data without authorisation. It also provides law enforcement bodies with greater investigative powers where persons can be ordered by the court to provide information to investigating officers. In addition, the Commonwealth Parliament recently passed the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004* to, among other things, outlaw credit card skimming. It also makes Internet banking fraud, including 'phishing', an offence. The penalty is up to five years' imprisonment.

Various other Commonwealth legislation contains offence provisions for identity related crimes such as the *Financial Transaction Reports Act 1988* and the *Financial Transaction Reports Regulations 1990* which create offences in relation to proof of identity for opening accounts with financial institutions. For example, it is an offence to open an account in a false name by tendering a false identification document.

In Queensland the main laws that cover identity fraud are provisions of the *Criminal Code 1899* (e.g. fraud (s 408C(1)); false pretences (s 427(1)); falsifying

records and producing false records (s 441); stealing (s 398); and misappropriation (s 408C)).

The existing Australian legislation is not consistent and varying definitions for the same sort of offence are used. There are also inconsistencies in the penalties that apply to the same type of offence in each jurisdiction.[44]

6.1.1 South Australian Legislation

The *Criminal Law Consolidation (Identity Theft) Amendment Act 2004* (SA) commenced on 5 September 2004. The Act amends the *Criminal Law Consolidation Act 1935* (SA) by inserting a new Part 5A to provide that a person who assumes a false identity of another person (whether living or dead, real or fictional, natural or corporate) makes a 'false pretence' to which the legislation applies, even if the person acts with the consent of the person whose identity is falsely assumed. The consequence is that a person who makes a false pretence intending to commit or facilitate the commission of a serious criminal offence (an indictable offence or a prescribed offence) is guilty of an offence. Thus, the conduct which is caught for the first time under Australian law is the conduct *before* the crime occurs that the identity theft intends to facilitate.

In addition, a person who makes use of another person's identification information intending, by doing so, to commit or facilitate the commission of a serious criminal offence, is guilty of an offence. 'Personal identification information' is broadly defined to include personal information such as name, date or place of birth, marital status *etcetera*, driver's licence or licence number, passport or passport number, biometric data, voice print, credit or debit card or number and the data stored or encrypted on it, any means commonly used by the person to identify himself or herself such as a digital signature, and numbers or letters used by the person as a way of personal identification. It does not matter if the person whose personal identification is used is living or dead or consents to the use of the information. In the case of a body corporate, such personal identification information can be its name, ABN, or the number of its bank account or credit card.

The penalty for the above offences is that which is appropriate to an attempt to commit the serious criminal offence in question.

It is also an offence for someone to produce or have possession of material (including personal identification information) that enables a person to assume a

---

[44] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', p 9.

false identity or to exercise a right of ownership to funds, credit, information or any other financial or non-financial benefit when it is intended to use that material for a criminal purpose. It is an offence to sell or give this material to another person knowing that the other person is likely to use it for a criminal purpose. The possession of equipment for making this type of material is also an offence. Such offences incur a maximum of three years' imprisonment.

An attempt has been made to narrow the scope of the legislation by providing that it does not apply to misrepresentations by persons under 18 for the purposes of obtaining alcohol or cigarettes or gaining entry to nightclubs *etcetera*. It is not the intention of this sort of law to catch under-age drinkers or deal with teenagers unlawfully entering an adult venue.[45]

After the court has found a person guilty of an offence, a victim of an identity fraud can apply for a certificate that details the offence and the name of the victim. This enables the victim to establish their credentials to avoid further adverse interaction with law enforcement authorities and prove that any crimes that come to light were not perpetrated by them.

6.1.2 United States

The main identity fraud legislation in the United States at the Federal level is the *Identity Theft and Assumption Deterrence (Identity Theft) Act 1998*. It is aimed at the creation, use or transfer of identification documents and also prohibits the theft or criminal use of personal information. It is unlawful for a person to knowingly transfer or use a means of identification of another person, without lawful authority, with the intention of committing any unlawful activity. It is also an offence to possess false or stolen identification documents with the intention to defraud and to produce, or have equipment used to produce, such false identification documents. The Act provides heavy penalties for certain types of identity fraud. For example, falsifying government issued identification information incurs a prison term of up to 15 years when it results in obtaining anything of value aggregating US$1,000 or more over a 12 month period. In other cases, prison for up to three years is standard. Note that if identity fraud is related to international terrorism, the offender can go to prison for up to 25 years. In addition, the legislation recognises individuals who have had their identity stolen to be victims, not just the banks and financial institutions.[46] However, given that

---

[45] Hon MJ Atkinson MP, Criminal Law Consolidation (Identity Theft) Amendment Bill 2004 (SA), Attorney-General, Second Reading Speech, *SA Hansard*, 15 October 2003.

[46] MJ Elston and SA Stein, 'International Cooperation in Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present', Computer Crime and Intellectual Property Section, US Department of Justice, November 2002, http://www.cybercrime.gov/.

identity theft and identity fraud continues to be a significant problem in the US, it is unclear how effective this legislation has been so far.[47]

Other Federal legislation aimed at identity fraud includes the *Fair and Accurate Credit Transactions Act 2003* which, among other things, obliges consumer reporting agencies to follow certain procedures about when to place, and how to respond to, fraud alerts on consumers' credit files; requires bodies issuing credit cards to adopt certain procedures if someone asks for an additional card where there was recently a change of address notification for the same account; requires businesses to give receipts *etcetera* of transactions alleged to be the result of identity fraud to the victim and authorised law enforcement bodies; and requires the truncation of credit card numbers on electronically printed receipts. The recently passed *Identity Theft Penalty Enhancement Act 2004* makes aggravated identity theft in conjunction with felonies (including immigration offences and bank fraud) a crime and establishes mandatory sentences. There is also legislation pending that is designed to assist victims of identity theft.[48]

At the State level, many jurisdictions have passed legislation dealing with the issue over the past five years.

6.1.3 Practical Difficulties of Obtaining Convictions under Legislation

Some commentators believe that effort should be directed at ensuring a reasonably uniform approach is taken to legislation in each jurisdiction, particularly in establishing key definitions of particular types of identity crime. This may cause less confusion in the area of law enforcement and prosecution, especially where the fraud crosses jurisdictions.[49]

There are others, who consider that it may be unnecessary to enact another piece of legislation to deal specifically with identity fraud as it is already covered by

---

47 D J Solove, 'The Legal Construction of Identity Theft', Paper presented to Symposium, Digital Cops in a Virtual Environment, Yale Law School, 26-28 March 2004. See also Roza Lozusic, 'Fraud and Identity Theft', *Briefing Paper 8/2003*, New South Wales Parliamentary Library, citing L LoPucki, 'Human Identification Theory and the Identity Theft Problem', *Texas Law Review*, 80(1) 2001, pp 89-134.

48 MS Smith, 'Internet Privacy: Overview and Pending Legislation', *Congressional Research Service Report for Congress*, updated 14 September 2004.

49 Australian Centre for Policing Research, 'Standardisation of Definitions of Identity Crime Terms', pp 6-7. See also RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', pp 7-12, where much of the above information concerning Commonwealth legislation was obtained.

existing laws. They consider that the real problem lies in the administration of the laws, not the laws themselves. It is this that needs to be improved.[50]

There are indeed considerable practical barriers to apprehending offenders in order to prosecute them even if there are laws to prosecute them under. Those who engage in identity fraud have highly sophisticated technological ways of obscuring their actual identities and avoiding detection, particularly if they live in another jurisdiction. Evidence is often difficult to obtain and collate and, in the end, resource implications may make pursuing the investigation unviable. This is exacerbated if it is necessary to extradite an offender from another country. Not only is this costly, there are attendant difficulties with obtaining cooperation from overseas authorities. If the extradition is successful, there is the legal issue of determining which law applies in a prosecution. Even if these problems are overcome, there is then the challenge of presenting highly complex and technical evidence to juries consisting of lay people who may have limited understanding of information technology and the way it is employed to perpetrate the complicated crimes under examination. Judges who preside over the trials must also have an understanding of the technology involved.[51]

Indeed, the most effective response measure may be risk management and fraud prevention. For instance, information networks between law enforcement agencies throughout the country or the world should be used so that contact can be made with an interjurisdictional counterpart once an investigation commences and information shared to assist investigations. The Australian Bureau of Criminal Intelligence has a secure Intranet to facilitate this. Such measures and better education of the public in protecting themselves from identity fraud may be the most effective combatants.[52]

6.2 GOVERNMENT POLICIES AND STRATEGIES

Much of the impetus for action by Government to counter identity fraud came from the House of Representatives Standing Committee *Numbers on the Run Report* in August 2000. In addition, there were other projects being undertaken considering the issue including an AUSTRAC working group on proof of identity; and the

---

[50] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', p 14.

[51] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', pp 15-17.

[52] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', pp 14-15.

Australian Bureau of Criminal Intelligence work on developing a national fraud analytical capacity to include information about identity fraud. The *Numbers on the Run Report* considered that an agency within the Attorney-General's portfolio should have responsibility for leading a Commonwealth Government response to identity fraud.[53] It also recommended that the Commonwealth should work with other Governments and industry to investigate and develop a national electronic gateway for document verification.[54]

In the agreement between the Commonwealth, States and Territories on terrorism and multi-jurisdictional crime on 5 April 2002, identity fraud was regarded as a priority issue. At the July 2004 meeting of the Standing Committee of Attorneys-General, endorsement was given for a common national framework for proof of identity from which all levels of Government can draw in developing their own models.[55]

Major Commonwealth Government initiatives, some in cooperation with the State and Territory Governments, include –

- The development of proposals for a common set of proof of identity documents of higher integrity to be used by government agencies and enhanced data matching across agencies (announced by the Minister for Justice and Customs on 6 July 2003). A feasibility study was commissioned into a possible online verification service that would allow the cross-checking of identification documents people produce to agencies to receive benefits and other services. The service would be developed in partnership with State and Territory Governments as it is those Governments which have responsibility for primary identification documents such as birth certificates and drivers' licences. It would link State and Federal agencies as data management improved.[56] The idea is to have a common set of high integrity identification documents; an online identity verification service for primary identification documents; and improved cross-agency data matching.

  The strategy is being guided by the work of the Commonwealth Reference Group on Identity Fraud which comprises a number of agencies including

---

53 *Numbers on the Run Report*, para 6.40.

54 *Numbers on the Run Report*, para 6.57.

55 Senator the Hon Christopher Ellison, 'Common Framework Endorsed to Fight Identity Fraud', *Media Statement*, 30 July 2004.

56 Senator the Hon Christopher Ellison, 'Identity fraud initiative to offer better protection for Australians', *Media Statement*, 6 July 2003. See http://www.crimeprevention.gov.au ('Identity Crime' button).

ASIO, AUSTRAC, the Australian Crime Commission, Attorney-General's Department, Centrelink, the Australian Customs Office, Department of Foreign Affairs and Trade, Department of Immigration, Multicultural and Indigenous Affairs, Department of Veterans' Affairs, Department of Family and Community Services, Department of Finance, Department of Health and Ageing and relevant State and Territory agencies. The Privacy Commissioner is involved in this 'electronic gateway' proposal to ensure that personal privacy is not unduly compromised.

- The AUSTRAC Steering Committee on Proof of Identity (comprising Commonwealth and State Government agencies that issue and use all types of proof of identity documents as well as law enforcement authorities, and financial services organisations) has, since its establishment in 1999, engaged in a series of projects regarding improvements to proof of identity processes in the public and private sectors.[57]

- Moves to upgrade passports by inserting a special computer chip that would be invulnerable to duplication. In May 2004, the Government allocated $2.2 million over the next 12 months to the Department of Foreign Affairs and Trade to test a prototype biometric passport for compatibility with US border control equipment.[58] If the trial is successful, the new passports should be introduced from the middle of 2005 at a cost of around $160 million.[59] Previously, in September 2003, new laws came into effect requiring those applying for a passport to produce more identification documentation and, if applying for one in any other name than that on their birth certificate, the person must officially change their name at the Register of Births Deaths and Marriages.[60] In December 2003, a laminated image of a 'floating kangaroo' for Australian passports was introduced in the attempt to deter forgeries.

  The Australian Passports Bill 2004 was introduced into the House of Representatives on 24 June 2004 (and re-introduced on 2 December 2004 after the Federal election) and is currently before the Commonwealth Parliament. It

---

57 S Cuganesan and D Lacey, pp 2-3.

58 Hon Alexander Downer MP, Minister for Foreign Affairs; Senator the Hon Amanda Vanstone, Minister for Immigration and Multicultural and Indigenous Affairs; Senator the Hon Christopher Ellison, Minister for Justice and Customs, 'Development of biometrics for border control', *Joint Media Statement*, 11 May 2004.

59 Cynthia Banham, 'US trip could require passport detour to Sydney', *Sydney Morning Herald* online, 20 December 2004.

60 Hon Alexander Downer MP, Minister for Foreign Affairs, 'New Measures to Enhance Security of Passport Issuing Process', *Media Statement*, 4 July 2003.

seeks to combat identity fraud relating to passports. It will increase penalties for passport fraud from $5,000 or two years' imprisonment to $100,000 or 10 years' imprisonment. It will clarify the Government's power to cancel or refuse a passport in various circumstances such as where the holder is likely to engage in, is charged with, or has been sentenced for, specific serious crimes such as sex tourism, drug trafficking, child abduction and terrorism. Various review rights and safeguards are built in. The Minister will be given the discretion to refuse to issue a passport to an applicant who has lost more than two passports in five years and higher fees may be imposed on serial 'losers' of passports. During 2003, Australians lost 30,000 passports. Provision will also be made for the introduction of facial biometric technology to enable better means of verifying identity.[61]

- Testing of face recognition technology (SmartGate) by the Australian Customs Office is being expanded over the next 12 months, backed by $3.1 million in Government funding. It is claimed that the use of biometrics, such as that occurring in this trial, will strengthen border protection because terrorists and other criminals will not be able to use fraudulently obtained passports to enter Australia without detection. Again, the Privacy Commissioner is involved in the development of the technology.[62] In the 2004-2005 Budget, the Commonwealth Government committed $9.7 million towards developing biometric technology to protect Australia's borders (which includes the abovementioned $3.1 million for the SmartGate trial).[63]

The involvement of the Privacy Commissioner in the development of ways to combat identity fraud recognises that certain measures may have privacy implications for individuals and their right not to have their personal information disclosed outside the agency to which it was given, except in limited circumstances. There is, indeed, some tension between the fact that a standardised process for identification and authentication of individuals may curtail identity fraud (noting that the theft of a person's identity to perpetrate such fraud is a significant invasion of privacy in itself), and ensuring that personal privacy rights are not unduly interfered with. Thus, measures to fight identity fraud must be designed to minimise the fear that Government and private organisations may unduly invade the personal privacy of individuals.[64] The challenge for policy

---

61 Hon Alexander Downer MP, Australian Passports Bill 2004 (Cth), Second Reading Speech, House of Representatives Hansard, 24 June 2004; Hon Alexander Downer MP, 'Passport Measures Help Secure Australia', *Media Statement*, 23 June 2004.

62 'Development of biometrics for border control', *Joint Media Statement*, 11 May 2004.

63 'Development of biometrics for border control', *Joint Media Statement*, 11 May 2004.

64 See, for example, G Main & B Robson, p 19.

makers is to properly balance personal privacy considerations against the broader public interest in guarding against identity fraud.

6.2.1 Law Enforcement

The Australian Crime Commission (ACC) provides intelligence to law enforcement agencies and investigators by keeping an Identity Fraud Register of suspect identities. A record of known identity fraud offenders is held on a central register rather than on the databases of individual agencies. The intention of the Register is to assist law enforcement agencies in determining if the same false identity has been used on other occasions, what assets are held in the fraudulent identity *etcetera*. Participating agencies can submit names to the Register but must first be satisfied, by undertaking relevant inquiries, that the identity details are actually fraudulent.

The Board of the ACC has approved a Special Intelligence Operation on Identity Fraud allowing the ACC to use coercive powers to assist identity fraud investigations where considered appropriate.[65] The ACC is also undertaking an intelligence operation into card skimming.

The High Tech Crime Centre formed in early 2003 brings together the Australian Federal Police (AFP) working with interstate and international counterparts to investigate computer related crimes that are serious, complex and/or cross jurisdictional boundaries. It will also work with the financial industry, including banks and credit card companies, to progress multi-jurisdictional investigations (see http://www.ahtcc.gov.au).

The Identity Crime Task Force (ICTF) was established in March 2003 comprising members of the AFP, ACC, Australian Customs Service, and the NSW Crime Commission with assistance from other departments such as the Department of Immigration, Multicultural and Indigenous Affairs, Department of Foreign Affairs, NSW Roads and Traffic Authority, and the Australian Taxation Office. In November 2003, it managed to break an identity fraud syndicate after Department of Immigration compliance officers alerted the AFP that they had allegedly found evidence of false documents during their search of a Sydney unit. AFP searches uncovered fraudulent identity documents (including 67 Medicare cards in various names, 20 passport photographs of different people, 13 blank NSW Road Traffic Authority change of address labels, and 7 Indonesian passports in various stages of alteration) and equipment to manufacture such documentation. Two Indonesian

---

[65] 'New report reveals identity fraud as a billion-dollar threat', *Media Statement*, 12 November 2003.

nationals were charged with identity fraud related offences under various Commonwealth legislation such as the *Criminal Code Act* and the *Passport Act*.[66]

Australasian Identity Crime Policing Strategy 2002-2005

In April 2002, Australasian Police Commissioners asked that an e-Crime Steering Committee examine identity crime and develop a national policing strategy. The policing strategy now aims to prevent and reduce identity crime and to assist its victims. The *Australasian Identity Crime Policing Strategy 2002-2005* was released in March 2003. It has six areas of focus which have objectives and a mix of activities geared at achieving a balance between prevention and effective responses to identity crime.[67] These focus areas are-

- Prevention – through a number of key activities including the efficient utilisation of police resources exploring the role that technology can play in assisting investigation; and contributing to sound research and statistical data. It is also recognised that identity crime is multi-jurisdictional and that the approach must be a coordinated one;
- Victim assistance – through efforts directed mainly at human victims (rather than traditional victims such as financial institutions and companies) to ensure that immediate and effective assistance is provided to them in terms of reporting the offence and provision of ongoing assistance and guidance;
- Partnerships with other law enforcement bodies as well as government and private agencies;
- Education and training for police and delivery of education to the community about identity crime;
- Effective resourcing and enforcement capacity to prevent, respond to and investigate identity crime; and
- Regulation and legislation – recognising that an effective legislative framework is needed to enable successful prosecution of identity theft and identity fraud and to allow victims to seek redress.

---

66 Australian Federal Police, 'Identity fraud syndicate arrested', *Media Release*, 12 November 2003.

67 Australasian Centre for Policing Research, *Australasian Identity Crime Policing Strategy 2002-2005 of the Police Commissioners' Conference*, Electronic Crime Steering Committee, March 2003.

6.3 TECHNOLOGICAL SOLUTIONS

The growing popularity of computers and Internet use has facilitated the escalation of identity fraud and its expansion across borders. Such technology also provides a means for offenders to remain anonymous or disguise their true identity. For example, many Internet Service Providers offer free email services where a person can just register using a false name and address.

Although e-commerce has become more popular and is supported by *Electronic Transaction Acts* in Australian jurisdictions, it has been reported that around 51% of small to medium size businesses are reluctant to engage in e-commerce until security is improved.[68] Indeed, even public key infrastructure can be compromised if a person registering for a pair of keys for use in secure online transactions uses a fake identity to register. Public key infrastructure enables transaction messages to be encrypted and one key is a private key kept by the sender of the encrypted data while the public key is sent to the other party in a secure manner, allowing the other party to decipher the information. So while the transaction might be secure from other people, one of the parties to the transaction holding the key to 'unlock' encrypted transaction data may be a fraudster.[69]

It has been claimed that Internet services that allow for the highest degrees of anonymity (e.g. encrypted email, Internet Relay Chat) are those most likely to be used for crimes, particularly online paedophilia and hacking.[70] Crime bodies also tend to operate out of countries where development of security technology is not a high priority.

Given the difficulty that legislators all over the world have with designing laws able to detect and prosecute online fraudsters, and the problems caused by territorial limitations of many laws, criminals often operate in countries with weaker laws.

---

[68] Comment by Julie Cleeland Nicholls of the Internet Service Provider, Pacific Internet, 'Online bank customers face 'phishing' fraud', *7.30 Report*, Transcript, 15 February 2004.

[69] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', p 2.

[70] RG Smith, 'Examining Legislative and Regulatory Controls on Identity Fraud in Australia', p 2, citing P Forde & H Armstrong, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, University of Plymouth, 16-18 July 2002.

6.3.1 Biometrics

An area that has been of great interest but is also somewhat controversial is biometric user authentication. This system enables identification of a person by way of unique physical properties such as fingerprints, retinal images or voice patterns. Hollywood movies and TV dramas set in US law enforcement agencies provide examples where an agent presses his or her eye against a scanner and the security door opens to allow them entry. Biometric user authentication is claimed to offer a higher level of integrity than standard password systems, knowledge based and token-based systems. Note that biometrics is essentially an authentication process and does not solve the problem of a false identification being used upon initial registration. However, while there may be benefits for identity security, biometric systems are very expensive and a number of privacy and confidentiality issues will have to be addressed.[71]

In June 2003, the Hong Kong Government commenced issuing new 'smart card' identification to its citizens to replace paper identification cards, a process anticipated to take four years. The aim is to crack down on illegal immigration. The smart cards carry a fingerprint biometric and the first persons to receive them include new arrivals to Hong Kong, persons turning 18 and persons applying for replacement cards or changing information on their existing cards. The cards are manufactured with material and laser engraving type printing that prevents forgery. The stored data on the cards is protected by cryptographic data so it cannot be altered or accessed by unauthorised persons. Users can, in most cases, add on other applications such as a driver's licence.[72]

Since the terrorist attacks on 11 September 2001, the United States and many other countries have become more concerned about national security. From 26 October 2004, the US Government has been issuing machine-readable, tamper resistant visas and similar documents using biometric identifiers to international visitors. Applicants aged between 14 and 80 seeking US visas are required to be fingerprinted. The biometric (two index fingers) is checked at the point of entry to ensure that the visa-holder is the same person who was issued the visa. The fingerprinting occurs as part of the application process and the electronic data from the fingerprints is stored in a database available to authorised US immigration officers. The idea is to improve the speed and integrity of identification of travellers and to protect the identity of the traveller while allowing for more secure

---

71 RG Smith, AIC, 'Addressing Identity-related Fraud', pp 12-13.

72 'Hong Kong Begins Issuing Smart Card IDs', June 2003, FindBiometrics, www.findbiometrics,com.

processing at points of entry.[73] Within the US, many Government agencies have begun using biometric authentication. Social service agencies in many US states have installed fingerprinting services.

Recently, the G8 member states, Britain, Canada, France Germany, Italy, Japan, the United States and Russia, agreed to develop a chip-based passport containing biometric data. A new requirement under the US visa waiver program makes it necessary for countries like Australia to issue passports with a facial recognition biometric identifier held on a microchip if they wish to remain in the program. As noted above, trials of the new biometric passports are underway in Australia with a decision on the uptake of the passports expected in May 2005. Travellers not in possession of such a passport will have to obtain a visa prior to arrival in the US.[74] The International Civil Aviation Organisation has adopted facial recognition as the global standard for biometric identifiers.[75]

There is, obviously, unease among those who fear incursions on individual privacy. Some fears have been raised about the potential misuse of the data by government but, of more concern is that, for all the promise for enhanced identification integrity, data from biometrics can be subject to unauthorised access. If a password is stolen, it can be revoked as a means of accessing money or benefits *etcetera* and a new one set up for the real owner. If a biometric characteristic (which, on a computer is stored in a data stream of binary numbers) is unlawfully accessed, it cannot be revoked because it is forever linked to the owner and will no longer be able to be used as authentication.[76] However, if used in conjunction with other identification systems and with regard to the privacy regime in Australia, biometrics can assist in tackling identity fraud.[77]

6.3.2 National Identity Cards

It is now technologically possible to create a single identity card for each Australian linked to a national database. Proposals for such have been discussed in many countries as a means of combating identity fraud. Since the September 11 terrorist attacks, more Western countries have begun considering electronic ID

---

73 Hong Kong United States Consulate, 'Biometric Collections Begin at Consulate General Hong Kong', *News Release*, 6 February 2004.

74 Cynthia Banham, 'US trip could require passport detour to Sydney'.

75 Karen Dearne, 'Canberra faces up to security', *Australian*, 24 February 2004, p 38.

76 G Mann & B Robson, p 31.

77 RG Smith, AIC, 'Addressing Identity-related Fraud', pp 13-14.

systems. It may, however, be difficult for Australians to accept the concept. While a single identity card could well provide the security of identity needed to facilitate the use of e-commerce and electronic government service delivery, the public may fear that the networked national database could be improperly accessed and identification data misused.[78] In the past there has been considerable public opposition to any proposal to introduce a national identity card. The classic example of this was the Australia Card idea in 1988 which was dropped in the face of public pressure.

There are already a number of 'smart cards' in existence that are designed for certain purposes. An example of this is the recent roll-out of Medicare 'smart cards' in Tasmania as part of the national program to implement electronic health records for patients who wish to have their key health information stored electronically and shared between health service providers. Brisbane, Sydney and Perth will start to, or have begun to, roll out 'smart cards' next year to link together bus, ferry and train tickets and to enable people to be able to set up an automatic transfer of funds from their bank accounts on a weekly or fortnightly basis to avoid having to pay daily fares. As yet, any decision about whether to link identity to the transit card is made by the individual card holder and any such link would not be biometric data.[79]

Federal Privacy Commissioner, Malcolm Crompton, considers that a 'smart card' could, if properly designed and used, actually improve personal privacy. However, the technology will have to be robust and used appropriately for people to accept it. A major concern is what Mr Crompton calls 'function creep' and uses the following example to illustrate the concept. You might now have a 'smart card' which has stored value contained on it to allow you to cross a major city tollway bridge more quickly and easily; tomorrow it might become compulsory to have your 'smart card' when you cross that same bridge; the next day the Government might state that all the traffic data on the use of the bridge can be used to improve traffic management in the city; then it becomes compulsory that all data can be accessed by the police with a warrant; then it is proposed that the police do not need a warrant to access the data.[80]

Mr Crompton also warned of the dangers involved in a system that would allow a lot of personal information to be easily put together electronically. Every person has considerable potentially identifying information about them held by government, business and other bodies. Examples are records of birth and

---

78 RG Smith, AIC, 'Addressing Identity-related Fraud', p 12.

79 D Baguley, 'Card sharps', *Bulletin with Newsweek*, No.6373, 20 May 2003, p 68.

80 D Baguley, p 68.

marriage certificates, drivers' licences, passports, visas, bank accounts, credit card numbers, name, address, vehicle registration details, tax file number, welfare benefit details, Medicare card number, employment details, health data, superannuation information *etcetera* as well as a myriad of publicly available information, such as telephone number, house sale price information and company share register information. There are also audit trails and data trails when using a computer such as the use of cookies by Websites and 'clickstream' data collected by some Internet marketeers.[81]

Mr Crompton notes that we are yet to feel the worst effects of data aggregation because it is currently difficult to link it all together properly due to difficulties and expense. At present, identifying information stored on individual government and private organisation databases tends to be kept in isolated 'silos' which is difficult to 'match' with information in other 'silos'. Data matching can be expensive also. Many people see benefits of bringing all of this information together and so avoid having to constantly provide evidence of identity, remember several passwords and PINs, and hold numerous cards. Governments argue that gathering more information about individuals protects against terrorism and helps to solve crimes more quickly. There are indeed benefits of such an approach but there are also potential risks that need to be managed.

The dangers of identity management through 'zipping' together all of a person's identification information are first, that the information could be misused by the organisation that has originally legitimately collected some of the data and, second, that the information (all conveniently packaged) could be stolen by hackers or through other means. Such technology could, instead of enhancing identity security, compromise it because it would allow a lot of information about a person to be stolen or misused. Any identity management tools must not only allow organisations to have confidence that they are dealing with the correct person (ie just bare identity not further personal information) but minimise inappropriate linkage of data and provide individuals with a reasonable level of control over what is known about them. Mr Crompton considers that there is strong evidence that good identity management can be delivered through technology. What is needed is for governments and organisations generally to ensure that identity management solutions do not, in combination, create unforeseen privacy consequences.[82]

It has also been argued that susceptibility to forgery of identification documents such as birth certificates and drivers' licences is best countered with making such

---

[81] M Crompton, Federal Privacy Commissioner, 'Proof of ID Required? Getting Identity Management Right', Australian IT Security Forum, 30 March 2004, pp 11ff.

[82] M Crompton, pp 13ff.

documents more robust rather than adding an additional layer of electronic authentication.[83]

The Commonwealth Government has ruled out introducing any national identity card. It is interesting to note, however, that the Australian public may be warming to the idea with a recent newspaper article reporting that a recent survey revealed that around 60% of Australians would welcome a national identity card.[84]

At a recent Asia-Pacific police conference in Canberra, the AFP's national manager for economic and special operations, Shane Connelly, said that there was evidence that identity fraud was used to facilitate terrorism operations including the September 11 attacks in the US and the bombing of the nightclub in Bali in 2002. In light of that, Mr Connolly said that Governments should now revisit the issue of a national identity card to assist in combating fraud and terrorism but keeping in mind privacy protection issues.[85] AFP Commissioner, Mick Keelty, regards the fight against identity related crime as one of the biggest issues facing law enforcement agencies given that it is an enabler to almost every form of organised criminal activity including terrorism and sexual servitude.[86]

The British Government proposes to introduce a compulsory identification card – the first in peacetime. In October 2004, the Home Secretary announced some refinements to the proposed card in response to comments made by the Home Affairs Select Committee's report on the ID card. It will be a single, universal ID card for all UK nationals incorporating biometrics and issued alongside passports. The scheme has been undergoing public consultation for some time and legislation will be introduced shortly to implement it during 2008.[87]

Malaysia has had a chip-based national identity card, driver's licence and passport since April 2001. There are plans to expand it to add applications like digital signatures for Internet transactions. It is optional for existing ID card holders but

---

83 C Britton, 'What's your identity?', Australian Consumers' Association, October 2003, http://www.choice.com.au.

84 Daryl Passmore, 'About turn on ID card', *Sunday Mail*, 28 December 2003, p 4.

85 James Riley, 'National ID cards urged in terror war', *Australian*, 15 October 2004.

86 Alison Rehn, 'ID fraud driving crime, terror', *Courier Mail*, 15 October 2004, p 3, citing Commissioner Keelty.

87 United Kingdom Home Office, 'Home Secretary Sets Out Next Steps on ID Cards', United Kingdom Passport Service News, 27 October 2004, http://www.passport.gov.uk.

compulsory for first time card holders or those seeking replacements and the plan is to embrace the entire Malaysian population within eight years.[88]

6.4 INDUSTRY AND GOVERNMENT AGENCY RESPONSES

In general, both business and government organisations need to ensure that they have, and that they maintain, various fraud prevention and fraud minimisation measures. Fraud prevention may involve fraud control policies with which all staff must be familiar and the use and upgrading of user authentication software for computer systems. Monitoring and other security procedures by IT sections of agencies and inter-agency data matching and networks to monitor transaction patterns are expensive and few agencies have been able to employ them to any large degree.[89] No less important, however, is the need to ensure adequate screening of personnel before they are employed. In addition, a relatively inexpensive practice that all businesses and government agencies should adopt is to train staff in how to spot a forgery or identity fraud.

Centrelink, for example, has an online service centre which requires identification and proof of identity to register and then provides the user (whose identity credentials are satisfactorily established) with a PIN and password to verify that they are the same person who has registered. Thus, persons applying for Centrelink payments must go through this identification and verification process and staff have training to enable them to ascertain whether identity documents produced by applicants are genuine: see www.centrelink.gov.au. A trial involving 2,500 clients is currently being undertaken by Centrelink to consider two matters – proof of the client's existence in Australia by birth certificate or citizenship certificate or visa, and how this identity has been used by the client in the community.[90]

Many businesses, financial institutions, and banks use the "100 points system" which is an identification verification procedure established under the *Financial Transactions Reports Act 1988* (Cth) and the *Financial Transactions Reports Regulations 1990* (Cth). The customer must produce certain primary documents (e.g. current passport and birth certificate) and secondary documents (e.g. driver's licence, employee ID card, Medicare card) and their importance or worth to establishing identity credentials is rated on a numerical point scale so that the total of the documents produced must equal or exceed 100 points. The "100 points

---

88 D Baguley, p 68.

89 RG Smith, AIC, 'Addressing Identity-related Fraud', p 9.

90 'Common Framework Endorsed to Fight Identity Fraud', *Media Statement*, 30 July 2004.

system" was developed long before many of the recent technological advancements. Most of the primary and secondary documents required can be counterfeited or forged.[91] The main issue is not so much the "100 points system" itself but the need to improve security features of the identity documents required and to train staff who inspect the documents for authenticity to be able to spot forgeries or counterfeits and to verify that the information contained in the documents with the issuing source.[92]

One security measure of recent development is Visa and MasterCard's specification program, EMV, which encourages banks to issue a chip card that is compliant with Visa's and MasterCard's rules. Most financial institutions and banks presently have public key infrastructure in place with a chip card being used for end to end encryption of the transaction data.[93]

Many government agencies providing benefits such as welfare payments and medical benefits run the risk of being defrauded. There could be improvements in State and Commonwealth inter-agency cooperation in checking and cross-validating identity documents. This could be along the lines of the current feasibility study into a possible online verification service that would allow the cross-checking by State, Territory and Commonwealth agencies of identification documents people produce to receive benefits and other services (examined above).[94]

An Authentication of External Clients Working Group is currently standardising identity documents in order to make documents used across agencies all the same.[95] For example, Centrelink could compare information about an applicant for a benefit with the Health Insurance Commission to verify that the person's family composition, address and other personal information match up. Privacy considerations are also relevant here. Usually, the process does not uncover identity fraud but, rather, oversights or changes in circumstances of applicants or recipients that might affect their entitlements.[96]

---

91 RG Smith, AIC, 'Addressing Identity-related Fraud', pp 10-11.

92 RG Smith, AIC, 'Addressing Identity-related Fraud', p 11.

93 D Curtis, p 67.

94 Senator the Hon Christopher Ellison, Minister for Justice and Customs, 'Identity fraud initiative to offer better protection for Australians', *Media Statement*, 6 July 2003.

95 Australian Government Information Management Office, 'Identification', at http://www.agimo.gov.au

96 Australian Parliament, Senate Community Affairs Legislation Committee (Budget Estimates), *Official Committee Hansard*, 4 June 2003, pp 443-448.

6.4.1 Superannuation

While it appears that identity fraud has not been a significant problem in the superannuation industry, the growth of superannuation funds in line with the ageing Australian population makes it an appealing target. For example, in the 2002-2003 financial year, ComSuper (the administrator of the Commonwealth public service superannuation funds) processed lump sum and pension payments of around $4.4 billion.[97] There has, however, been one distressing example in Victoria of four people aged over 55 having their superannuation funds stolen to the value of $612,000. The criminal assumed the identity of each victim and sent false identification documents to the superannuation fund requesting a payout of benefit. The payout occurred by way of cheques being forwarded to the offender.[98]

A partner with Deloitte Touché Tohmatsu, Richard Rassi, considers that the industry should take proactive measures to protect against potential fraud including making sure that there are strong controls around processing of, and requesting, benefit payments and ensuring that there is enough evidence to verify the identity of the individual recipient.

ComSuper apparently has a number of security measures for requiring verification before benefits are obtained, including the following checks regarding benefit applications from retiring contributors:

- requiring a departmental report before the benefit is processed;
- requiring that the employer sends an electronic notification verifying that a member has ceased employment;
- ensuring that the systems alert ComSuper if contributions continue to come in after the benefit has been processed; and
- requiring that benefit applications are signed (and the signature is compared with that on file).

The benefit must be paid into a bank account and the recipient has to go through a "100 point identity check" to create that account with the bank.

ComSuper also has systems in place to conduct 'life surveys' on high risk members such as those over 90 years old. It also restricts staff access to tax file numbers; requires that approval of payments is a two-stage process involving two people; and its systems, processes and who is able to access them are subject to regular audit. In addition, there is consideration being given to introducing monthly data

---

97 K Power, 'Pilfering', Management Issues, *Superfunds*, November 2003, pp 34-36, p 34.

98 S Ringin, p 78.

matching of ComSuper's records with those held at Births Deaths and Marriages to identify deaths of members.[99]

It is also important for members to exercise caution by checking their statements for any anomalies. Ultimately, if a member is defrauded, it might be difficult for him or her to overcome the problems and redeem the loss.

6.5 WORKPLACES GENERALLY

Organisations must have codes of conduct for computer and Internet use by their employees and security and authentication systems, such as passwords and user IDs, to access them. Computer use needs to be monitored. While many organisations leave it up to the IT section to develop security solutions, the IT section must have accurate and proper feedback from the entire organisation and be involved in decision making that has information technology implications.[100]

While one thinks of identity fraud being committed from outside an organisation, the sad reality is that there have been many instances of fraud from within – by employees. As well as technological audits of security and other computer software, simple measures can be taken to protect information. There may be employees who undergo a significant change of lifestyle such as expensive cars or holidays. There needs to be training in organisations about how to detect high risk employees.[101] Moreover, careful checks need to be made when an employee is first appointed.

6.6 CONSUMERS

As part of the Commonwealth Government's *National Crime Prevention Program – Towards a Safer Australia*, an *Identity Theft Kit* was recently launched with the aim of helping Australians prevent and respond to identity theft. Some tips for consumers to minimise their exposure to identity fraud, together with some suggested in the *Identity Theft Kit*, include –

- Carefully check bank and credit card statements and phone accounts and promptly report any discrepancies or suspicious transactions to the credit or finance provider or the utility.

---

99 K Power, p 35.

100 C Gill, p 44.

101 C Gill, p 44, citing a Fraud Risk Services Director from Ernst & Young.

- Do not have cheque books and credit or debit cards sent to you through the mail. Arrange to collect them from the bank in person.

- Make sure that your letter box is lockable and is large enough to contain all mail you are likely to receive so that important personal information is not left sticking out or on top. If you seem to not be receiving mail or there is a drop in volume, check with the post office. Someone might have filled in a change of address form in your name!

- Do not share identifying information with anyone that you do not trust or has not satisfied you of their *bona fides*. With phone marketeers or phone callers alleging to represent charities, it is easy to fall into a trap of providing the caller with your credit card number to secure a holiday or make a donation. This should not be done over the telephone as there is no way of knowing who the caller actually is. If the caller seeks personal information always ask what it is being used for and how it will be used (as in most cases, the Commonwealth *Privacy Act 1988* will protect the collection and use of your personal information).

- Protect all important credit card and bank accounts as well as phone accounts with a password – and avoid using obvious passwords or the same one on all accounts. Do not keep the passwords near the accounts or store them on a computer.

- To avoid becoming a victim of 'phishing', beware of emails purporting to be from financial institutions or banks that ask you to confirm your password or account number. Banks and financial institutions would not make such a request as they hold those details internally.[102] If there is a link to the bank website in the email, avoid clicking on it as it might take you to a sham website enticing you to enter your username and password which is then captured by the online scammer.[103]

- Put a limit on the amount of credit in your accounts so that the loss is contained if the card is stolen.

- Never throw out any paperwork that contains your personal information (e.g. bank account statements, any documents that state your date of birth) into your rubbish bin (thieves are aware that people attempt to 'do the right thing' and place paper in the recycle bin) without shredding, cutting or burning first.

---

[102] Queensland Office of Fair Trading, Common Scams: 'Bogus bank emails', 16 March 2004.

[103] Advice given in an interview with Alistair MacGibbon, head of the High Tech Crime Centre, 'Online bank customers face 'phishing' fraud', Transcript, *7.30 Report*, 5 May 2004, http://www.abc.net.au/7.30

- When you have visitors to your home, do not leave documents that contain your personal information lying about. Take particular care if you share a house or have cleaners or child minders come to your home. Similarly, at work, make sure you do not leave such information or passwords *etcetera* in obvious locations (e.g. a drawer in your desk) or on your computer without password protection. An identity thief can be someone you know or a work colleague. A Townsville man used his younger brother's driver's licence details when charged with drink driving and speeding offences. It took the brother many years to prove he was not at fault and clear his name.[104] Recent studies in the United States found that up to 17% of victims knew the offender.[105]

- If you lose your purse, wallet or credit cards, or they are stolen, report this immediately to the bank or credit card provider so that all cards and accounts can be cancelled or frozen. The police should also be notified as a thief or finder of the items might use your identity to commit crimes.

- Make identity theft through your personal computer harder by using and regularly changing passwords; upgrade virus protection programs and other protection software; use a firewall to prevent unauthorised access to the computer; make sure you delete all personal information from the hard drive before you sell or dispose of your computer (there are programs available that will do this); and be wary of using public access computers in libraries or cafes to access financial or other personal documents or anything requiring a password.

- If you keep receiving unsolicited mail, contact the company and ask that your name be removed from their mailing lists.

- Baycorp Advantage at www.baycorpadvantage.com.au allows you to review your credit file and it also provides a service where, on subscribing, you can be notified of any changes to your file.[106] Consumers should order a copy of their credit report regularly so that unauthorised activity can be detected quickly.

The *Identity Theft Kit* also has information for victims of identity theft. It advises that as soon as you realise that personal information has been stolen or money is

---

104 Lou Robson, p 47.

105 USA, Identity Theft Resource Centre, *Identity Theft: The Aftermath 2003*, p 21, citing California Public Interest Research Group and Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft – A Survey of Identity Theft Victims and Recommendations for Reform*, May 2000.

106 S Ringin, p 81.

missing from your account, report it to the police immediately. If asked to do so, provide the police with relevant documentation, such as bank statements, to assist in more rapid detection. It is also important to inform the credit reporting agency (e.g. Baycorp Advantage) that you are a victim of identity theft so an alert can be placed on your file which will make you aware if new accounts are opened in your name. You should ensure you receive a copy of your new credit file which should be carefully examined by you. Contact credit providers to request that unauthorised accounts in your name be closed and then inform the credit reporting agency. There may also be other measures that need to be taken which should be investigated with the providers or the credit reporting agency. The Kit provides advice about clearing criminal records in the victim's name and having the victim's name removed from the offenders' database.

RECENT PARLIAMENTARY LIBRARY RESEARCH PUBLICATIONS 2005

RESEARCH BRIEFS

RBR2005/01	*Standards for Young Workers: The Industrial Relations (Minimum Employment Age) Amendment Bill 2004 (Qld)*	Feb 2005
RBR2005/02	*Financial Literacy in Queensland: Bankruptcy Trends and Government Initiatives*	Feb 2005
RBR2005/03	*Identity Fraud*	Feb 2005

Research Papers are available as PDF files:

- *to members of the general public the full text of Research briefs is now available on the parliamentary web site, URL, http://www.parliament.qld.gov.au/Parlib/Publications/publications.htm*
- *http://www.parliament.qld.gov.au/Library/Query.exe* – e-Documents & e-Articles – Quick display of Library's research publications

A Subject Index to Research Publications is available at the following site: http://www.parliament.qld.gov.au/Parlib/Publications/bysubject.htm
Parliamentary Library - Research Publications & Resources Telephone (07) 3406 7108
Orders may be sent to Carissa Griggs, carissa.griggs@parliament.qld.gov.au

This Publication:

RBR 2005/03 ***Identity Fraud*** **(QPL, February 2005)**