NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Fraud and Identity Theft

by

Roza Lozusic

Briefing Paper No 8/03

RELATED PUBLICATIONS

- Private sector fraud in New South Wales: incidence and regulation by Rachel Simpson, Briefing Paper No 18/97

ISSN 1325-5142
ISBN 0-7313-1733-5

May 2003

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

David Clune (MA, PhD, Dip Lib), Manager..... (02) 9230 2484

Gareth Griffith (BSc (Econ) (Hons), LLB (Hons), PhD),
Senior Research Officer, Politics and Government / Law ..... (02) 9230 2356

Talina Drabsch (BA, LLB (Hons)), Research Officer, Law..... (02) 9230 2768

Rowena Johns (BA (Hons), LLB), Research Officer, Law..... (02) 9230 2003

Roza Lozusic (BA, LLB), Research Officer, Law ..... (02) 9230 3085

Stewart Smith (BSc (Hons), MELGL), Research Officer, Environment ... (02) 9230 2798

John Wilkinson (BA (Hons), MA), Research Officer, Economics ..... (02) 9230 2006

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:

www.parliament.nsw.gov.au/WEB_FEED/PHWebContent.nsf/PHPages/LibraryPublications

CONTENTS

EXECUTIVE SUMMARY

Fraud is reportedly one of the fastest growing crimes in Australia. According to the Australian Institute of Criminology, the estimated cost of fraud to Australia is in excess of $5 billion a year, which represents almost a third of the total cost of crime in Australia ($19 billion).

Identity fraud, in particular, where identities are stolen or fictitious identities are created, is becoming an increasing problem due to emerging (and rapidly evolving) technologies which enable such crimes to be committed. Not only does identity fraud pose a significant financial cost to the community (with estimates ranging from $2 billion to $3.5 billion a year) but it impacts significantly on: victims (whose identities have been stolen); financial and other institutions; and law enforcement agencies because of the difficulty in tackling such crime, and because identity fraud facilitates the commission of other types of crime such as people smuggling.

Section 2 of this paper deals with the subject of fraud in general, including the definition of fraud and identity fraud, the types of fraud, perpetrators of fraud, and the magnitude of fraud in Australia. This latter area incorporates the latest figures from the *KPMG Fraud Survey 2002*. (pp 2-11)

Section 3 deals with identity fraud. It includes a discussion of factors that influence identity fraud, how it is perpetrated, and the magnitude of the problem in Australia as well as examples of identity fraud and theft. (pp 11-17)

Section 4 outlines briefly some of the crime statistics in this area. (p18) Appendix A contains tables of crimes statistics referred to in section 4.

Section 5 looks at legislative and other responses to the problem of fraud. It outlines NSW, Federal and other responses. (pp 19-28)

Section 6 outlines some of the law enforcement initiatives in this area by: the New South Wales Police; the New South Wales Crime Commission; and the Australian Federal Police.

Finally, Section 7 contains a range of private sector views and responses to the issue of fraud and identity fraud. (pp 32-39)

1. INTRODUCTION

There has been a rapid increase in the level of fraud in recent years and, in particular, a significant growing problem of identity fraud and identity theft. Identity theft is reportedly "the fastest growing crime in Australia."[1] For victims of identity theft the impact can be devastating – both financially and in reputation. They can be caught in a tangled web[2], having to prove their own identity and re-establish their reputation and credit-worthiness.

Not only can its impact be felt on consumers, but fraud also has a significant financial impact on the private and public sector and the community in general. There have been various estimates of the financial cost of fraud – although it has been noted that such figures can at best be only a guess. It has been estimated that fraud, in general, costs between $3 billion and $5 billion a year in Australia[3], and that identity theft is estimated to cost $2 billion a year in Australia alone[4] (although some estimates of the cost of identity fraud alone put the figure as high as $3.5 billion). According to the KPMG *Fraud Survey 2002*, fraud cost a collective $273 million to the respondents of the survey[5] in the 1999/2001 period (October to September).[6] Recent AIC figures state that the cost of fraud was almost a third of the total cost of crime.

The New South Wales Crime Commission has commented on the problem and cost of identity fraud. It has stated in its latest annual report that "Identity fraud, through either

---

1 "Police, help, they took my identity", *Sydney Morning Herald*, 28/2/03.

2 Hemphill T, "Identity Theft: A Cost of Business? *Business and Society Review*, 106 No 1, Spring 2001, p 52. Hemphill cites the predicament faced by a journalist in the US, Stacy Sullivan, when her identity was stolen. According to Hemphill, she described (in an opinion piece for the *New York Times*), the extreme difficulty she faced in trying to re-establish her identity and reputation including the "Kafkaesque maze" she had to negotiate in order to do so. After four years Ms Sullivan still had unpaid bills reflected on her credit report and she was unable to rent an apartment. Hemphill notes that "there are acute personal losses reflected in this privacy violation...[of identity theft]...that thereafter affects an individual's everyday life".

3 Dearne K, "ID card would 'curb fraud'", *Australian IT*, 12/11/02, available at http://www.australianit.news.com.au. The figures ($3 to $3.5 billion) are from Australian Federal Police estimates. New South Wales Crime Commission, *Annual Report 2001/02*, p 21. Although it has been noted by the AIC that dollar figures at best can only be a rough estimate. The latest $5 billion estimate was reported in a recent AIC publication: Mayhew P, *Counting the Costs of Crime in Australia*, trends & issues in crime and criminal justice No 247, April 2003, p 5. See this publication for a discussion on the difficulties with estimating the cost of fraud as well as: Mayhew P, *Counting the Costs of Crime in Australia: Technical Report*, AIC Technical and Background paper Series No 4, April 2003, pp56-62.

4 AIC, "Identity Fraud", *Australian Institute of Criminology Newsletter*, Summer/Autumn 2002, no 17, p 3.

5 Large private and public sector organisations.

6 KPMG, *Fraud Survey 2002*, p i.

identity manufacturing or identity theft, is used extensively to facilitate crime, avoid detection, conceal the proceeds of crime and avoid tax. It is estimated to cost the Australian community more than $3.5 billion annually. Anecdotal evidence indicates that this cost will increase significantly in coming years if no effective action is taken."[7]

Fraud is not simply a national problem, fraud crosses national borders and the by-products of fraud (such as false identification for example) enable other crimes to be committed (such as people smuggling). Due to the often high-tech way in which fraud can be committed, it poses enormous difficulties for law enforcement agencies.

The Australian Institute of Criminology (AIC) has stated "the prevention and control of fraud are two of the great challenges for Australia now, and in the years to come."[8]

It has been argued that the increase in fraud, and in particular identity fraud and identity theft, is undoubtedly linked to technological advances. There are convincing arguments that the subsequent erosion of privacy, which has resulted from these technological advances, has facilitated an environment where such crime can be easily and readily committed.[9]

Many reports and papers have been published on the subject in recent years. An earlier *Briefing Paper*, "Private sector fraud in New South Wales: incidence and regulation", was published in 1997[10]. This paper is an update of that, but with a focus on the emerging problem of identity fraud. This paper will also look at government, law enforcement, private sector and policy responses to the issue of identity fraud and theft.

2. FRAUD IN GENERAL

Definition of fraud and identity fraud

Due to its wide-ranging nature, fraud is not simple to define. Nonetheless the Australian Institute of Criminology (AIC) has noted that fraud is a crime that "involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone

---

7 New South Wales Crime Commission, *Annual Report 2001/02*, p 21.

8 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*. Some of the reasons for this is that such high-tech crime brings with it "complex jurisdictional and technical issues, especially if the victim and offender are in different places, and the money has been moved at the speed of light through cyberspace" (p 2 of 12, internet download).

9 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502. Mike Hatch is the Minnesota Attorney General. p 12 of internet download.

10 Simpson R, "Private sector fraud in New South Wales: incidence and regulation", *Briefing Paper 18/97*, NSW Parliamentary Library Research Service, 1997

else".[11]

As noted in the earlier *Briefing Paper*, in terms of the criminal law, fraud itself is not an offence in NSW. Instead there are many criminal offences that contain elements of fraud. The Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (MCCOC) examined the question of what constitutes fraud in detail. In their 1995 report they identified a basic fraud offence as containing the following elements:

1. By any deception
2. Dishonestly
3. Obtains
4. Property
5. Belonging to another
6. Intent to permanently deprive.[12]

Identity fraud (as distinguished from fraud in general) incorporates the above elements but also encompasses two specific types of fraud: identity theft, where an *existing* identity is stolen/used; and identity fraud in general, where a new identity is *created* in order to obtain a financial or other benefit of some kind.[13]

Legal Framework

Fraudulent offences can be statute[14] or common law based criminal offences in federal and state criminal jurisdictions[15]. Indeed, there are a multitude of offences which can fall within the category of fraudulent offences – a central element of which includes acting with dishonesty or deception. As noted in the earlier *Briefing Paper*, fraud itself is not an offence in NSW. Instead there are many different offences which can fall within the category of fraud.

New South Wales and South Australia are the only two states in Australia that retain the common law approach to fraud regulation[16]. The common law approach is based on the

---

11 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*.

12 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Model Criminal Code: Chapter 3, Theft, Fraud, Bribery and Related Offences*, December 1995, p 137. As cited by Simpson R, op cit n 10, p 3.

13 As Hemphill describes "'Identity fraud' is a much for inclusive category than identity theft". op cit n 2, p 61.

14 The relevant criminal law statutes in the various jurisdictions within Australia apply. The relevant legislation in NSW being the *Crimes Act 1900* (NSW), in particular Part 4 (offences relating to property), Division 1 (stealing and like offences), and Subdivisions: 8 (fraudulent misappropriation); 9 (valueless cheques); 10 (obtaining money by deception); 11 (obtaining money by false or misleading statements); 12 (obtaining credit by fraud); 13 (false pretences); and 14 (fraudulent arrangements).

15 In addition, civil remedies may be available. See further below.

16 As noted by Simpson "The common law approach is contained in the *Griffiths Code*, in

offence of larceny, which is modified and supplemented by a large number of statutory offences (which in NSW are contained in the *Crimes Act 1900* (NSW)).

Six broad categories of offences can be identified as coming under the umbrella of fraud:[17]

1. Bribery
2. Conflict of interest
3. False statements and false claims
   - The offences that fall within this category are very relevant in the context of this paper. This category of offences is primarily regulated by the *Crimes Act 1900* (NSW), for example: obtaining money etc by deception (s178BA); obtaining money by false or misleading statements (s178BB); obtaining credit by fraud (s178C); false pretences (s179); and inducing persons into entering certain arrangements through fraudulent statements (s185A).
4. Extortion
5. Fraudulent conversion
6. Embezzlement

These categories are reflected in the crime statistics collated in this state by the New South Wales Bureau of Crime Statistics and Research (BOCSAR) in which the number of charges and range of penalties for fraud offences[18] come under the heading of "deception and other related offences". The five categories listed under this heading are:

- Fraud, forgery or false financial instruments
- Counterfeiting currency and related offences
- Dishonest conversion
- Bribery
- Other deception offences.

Criminal incidents[19] are listed/collated as "Recorded criminal incidents for fraud". For further information on crime statistics on fraud see the section on Crime Statistics at Section 4 of this paper.[20]

---

which the various forms of stealing were combined into one offence of stealing. Stealing is defined to include fraudulent taking and fraudulent conversion. The code draws a distinction between stealing and other forms of fraud eg false pretences, so its value as a simplifying mechanism for the common law is limited (MCCOC, p 2). The *Griffiths Code* was replaced in England by the *Theft Act 1968* which was based on three main offences: theft, obtaining property by deception and obtaining a financial advantage by deception."

17 For more information and detail (such as judicial decisions) on the definition of fraud and fraudulent offences see the earlier *Briefing Paper*, op cit n 10, pp 2-10.

18 In both lower and higher courts.

19 Obtained from data that is extracted from the NSW Police Service's Computerised Operational Policing System database (COPS). The data is collated by BOCSAR.

20 For further information on crime statistics on fraud see the section on Crime Statistics at Section 4 of this paper.

Whilst various offences can fall within the broad category of fraud, identity theft itself is not an offence in NSW, nor in other jurisdictions within Australia. To date the only jurisdiction within Australia to announce proposed legislation to target identity theft specifically (ie to make it a crime) is South Australia.[21]

Although fraud largely falls within the criminal law, the commencement of civil action (so as to obtain civil remedies such as damages) can be used as an alternative (or in addition) to criminal prosecution. Civil action can provide significant benefits over criminal prosecution due to the lower standard of proof required - on the balance of probabilities[22] as opposed to beyond reasonable doubt. As noted by Graycar:

> Given the difficulties in prosecuting fraud, there has been an increasing reliance in recent years placed on civil remedies as a complement or as an alternative to criminal prosecution. In contrast to the criminal law, which requires proof beyond reasonable doubt of intent to defraud, civil remedies only require proof on the balance of probabilities. Civil actions have prevailed not only against the perpetrators of fraud, but also against auditors who have been found negligent in the performance of the audit function. The quantum of damages which might follow a successful civil action could be formidable, and act as a significant deterrent, at least where it is possible to gain access to sizeable assets. Civil remedies also provide for a degree of compensation to the victim which might not otherwise flow from the criminal process.[23]

Types of fraud

Fraud is often categorised by the industry in which the fraud has occurred (eg insurance fraud) but it can also be categorised by the type of fraud (eg credit card fraud).

Not only is there a wide variety in the types of fraud that can be committed but also, as noted by the AIC, there are enormously diverse ranges of circumstances in which fraud can exist. These include:

Fraud by industry eg private sector:

- financial services sector fraud (which encompasses many types of fraud such as credit card (and other card) fraud, cheque fraud and other identity related fraud)

---

21 According to the SA Premier, Mike Rann, in his media release: "Crackdown on identity Theft", *Media Release*, 25/2/03. For more information see further below.

22 Proving something on the balance of probabilities means that a plaintiff has to provide sufficient evidence which would show that their version of events is more probable than not. *Butterworths Australian Legal Dictionary*, 1997.

23 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*. (p 5 of 12 from internet download)

- insurance fraud
- telecommunications fraud
- superannuation fraud
- securities fraud
- computer fraud

Also public sector fraud – which includes fraud committed against the government and public sector agencies for example:

- migration fraud
- health care/benefits (ie medicare) fraud
- taxation fraud
- welfare fraud

In terms of financial services sector fraud, the most common types include: transaction fraud such as credit card (and other card) fraud, obtaining finance by deception and cheque related fraud; and identity-related fraud.[24]

Who commits fraud?

This question can be assessed and answered in different ways: in terms of the relationship of the perpetrator to the victim (victim in this sense generally meaning the organisation which has been defrauded); or in terms of the individual characteristics of such perpetrators.

With respect to the former, the relationship of the perpetrator to the victim, the type of fraud that seems to be prevalent in private and public sector organisations (in terms of the total cost to an organisation) is that which is committed by external parties.[25] However, fraud committed by internal parties (such as employees, management etc) is also a significant problem. For example, the Australian Institute of Criminology (AIC) has previously noted that the majority of fraud offences in the private sector are committed by internal parties such as employees and management,[26] although a more recent study by the AIC showed that, of the cases in the sample studied, almost one-third (30%) of accused persons had some form of employment relationship with their victim.[27]

In an AIC *trends & issues* paper, Grabosky and Duffield, outline four categories of fraud defined by the perpetrator and their relationship with the victim:

---

24 Chapman A & Smith R, "Controlling Financial Services Fraud", *trends & issues in crime and criminal justice No 189*, Australian Institute of Criminology, February 2001, pp 2-3.

25 For example, in the KPMG *Fraud Survey 2002*, it was found that approximately 50% of the fraud that was reported was credit card fraud against banks. These involved the use of stolen credit cards or credit card numbers that were fraudulently manufactured. (p i)

26 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August* 2000, p 4.

27 AIC & PricewaterhouseCoopers, *Serious Fraud in Australia and New Zealand*, 2003, AIC Research and Public Policy Serious No 48, pp38-42.

- Fraud committed by a senior official or principal of an organisation against that organisation (eg entrepreneurs)
- Fraud committed by a client or employee of an organisation. (eg insurance fraud, embezzlement, tax evasion)
- Fraud committed by one individual against another in a face to face transaction (eg fraudulent investment advisers)
- Fraud committed against a number of individuals through print or media (eg Nigerian advance fee frauds).[28]

To the above list we can also add fraud that is committed against an individual by an unknown individual (or criminal gang), for example such as in the case of identity fraud and theft or credit card fraud.

With respect to the individual characteristics of perpetrators of fraud, a recent AIC report found that the majority of offenders were born in Australia (66%), tended to be older (mid 40s), male and had completed secondary education or had professional qualifications. Of those who were not born in Australia, they were mainly from Asian or Southern European background.[29]

Who are the victims of fraud?
The victims of fraud include organisations and individuals/consumers (particularly in cases of identity theft).

Responsibility for fraud
Responsibility for the prevention, detection and enforcement of fraud lies with a mix of law enforcement agencies, at both a federal and state level, as well as public and private sector organisations. In addition, private sector (and other) organisations can employ (or retain the services of) investigators to conduct internal inquiries/investigations into fraudulent activity that occurs within their organisations.

Magnitude of fraud in Australia
In their report, *Fraud Survey 2002* ('the Survey'), KPMG outline their findings with respect to the magnitude of fraud amongst the organisations surveyed within Australia and New Zealand – in both public and private sectors. The survey was sent to 2,000 of the largest organisations – 361 responded.[30]

---

28 Grabosky P and Duffield G, "Red Flags of Fraud", *trends & issues in crime and criminal justice No 200*, March 2001, p 1.

29 AIC & PricewaterhouseCoopers, op cit n 27, pp 34 & 64. For further information about the characteristics of individuals who commit fraud see this report at pp 34-42 and summary on p 4 & 64.

30 KPMG, *Fraud Survey 2002*, p i. The size of the respondents' organisation is reflected in the fact that 70% of the respondents had a gross revenue of more than $100 million Australian dollars, with 22% earning over $500 million. 83% of the respondents also employed over 100 employees with 29% of the respondents employing more than a 1000 employees (p 2).

The findings look at the scope of fraud perpetrated by external parties and the cost to private sector organisations. The other types of fraud discussed are internal in nature and involve fraud committed by internal management and non-management employees. They noted that:

> Since the 1999 survey, a number of alarming commercial crime trends have emerged with the Australian and New Zealand economies including:
>
> - an increase in the involvement of criminal gangs in external fraudulent attacks on financial institutions by using stolen cheques and falsified identification, including drivers' licences;
> - an increase in the incidence of international criminals coming into Australia and New Zealand, committing major fraud and then leaving with the proceeds of their crimes; and
> - the development of ever more ingenious methods for manipulating cheques and other negotiable instruments, including the removal or alteration of payee and amount.

In their summary of major findings they noted:

> - the 361 respondents lost a total of $273 million to fraudulent conduct in the survey period...
> - 44,654 instances were reported (approximately 50% of these were credit card fraud against banks, involving the use of stolen credit cards or fraudulently manufactured credit card numbers)...
> - more than $30 million was lost to fraud in off-shore operations, an increase of more than 100% over the loss reported in the 1999 survey.[31]

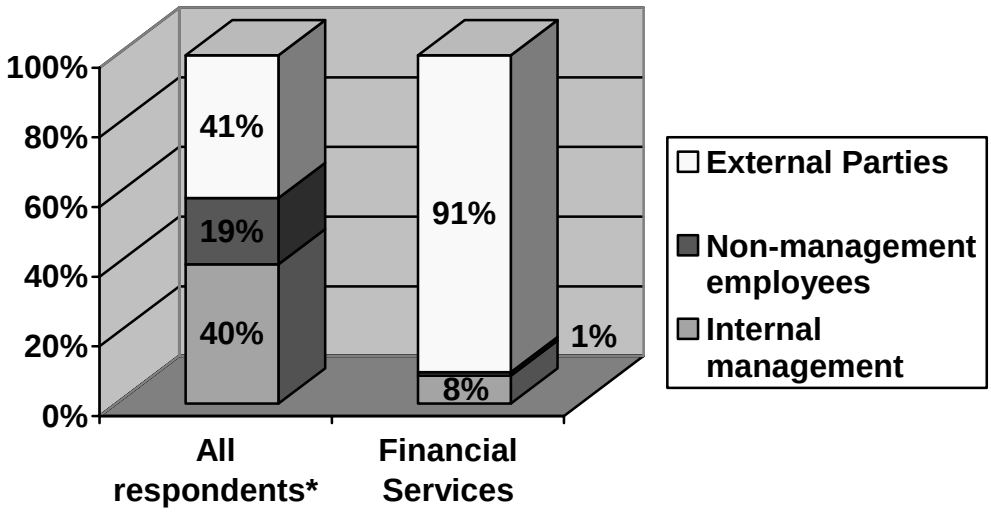
In its report KPMG note that "fraud in the financial services sector is heavily weighted towards external parties, which is mainly due to the large number of credit card frauds, services and benefits obtained by false information, and cheque forgery (a significant increase from the 1999 survey)."[32]

---

31 ibid. p i.

32 KPMG, *Fraud Survey 2002*, p 5

For example the following chart is an analysis of fraud by value reproduced from the Survey:



*** excluding external financial services fraud**

The chart shows that in the financial services sector, external parties are responsible for the great majority (91%) of the total value of fraud.

When separated by perpetrator types, the average loss per organisation where external parties commit fraud is significantly higher that that perpetrated by internal parties.

	Average value per fraud reported	Average loss per organisation
Perpetrator type		
Internal management	$96,732	$434,664
Non-management employees	$18,118	$132,277
External parties	$3,585	$2,222,798

For detail on crime statistics see Section 4 below.

A recent report by the Australian Institute of Criminology (AIC), in conjunction with PricewaterhouseCoopers, made the following key findings with respect to the magnitude of fraud in Australia:

- The most common type of fraud involved obtaining finance or credit by deception (21%). This was followed by fraud that involved cheques (15%).
- Most cases involved fraud that was perpetrated against organisations as opposed to individuals. The largest number of cases involved victims who were organisations located within the financial services sector (36%). The report notes that "The financial services sector was the most victimised group largely because the most frequently occurring type of fraud involved abuse of credit and financial products."

- False documents were used in 69% of cases.
- Identity fraud was evident in a significant proportion of cases (in 36% of files). Stolen identities were used in 13% of files and false identities were used in approximately 25% of files.
- Of the 155 files examined...[which were completed files from police and prosecution agencies in Australia and New Zealand]...there were recorded losses of $260.5 million. $13.5 million was recovered at the time of sentencing. The total amount of actual loss suffered was $143.9 million.[33]
- The main methods in which proceeds of crime were disposed of were: purchasing of luxurious goods and services (eg motor vehicles or travel); and expenditure on gambling and personal living expenses. The report notes "this reflected the fact that greed was the most prevalent motivation of offenders (27% of offenders) followed by gambling (16%)".[34]

The AIC notes, with respect to recent history of fraud:

> During the early 1990s, there was a decline...[in fraud]..., which may be due to the effects of various fraud control initiatives taken by some public and private sector agencies such as the insurance industry. Over the last few years, however, the rate has again begun to increase which may indicate a greater willingness to report fraud to the police, as already mentioned. These trends may also, of course, reflect changes in the underlying incidence of fraud in the community.[35]

Even though there have been various studies (such as private sector surveys) which have attempted to quantify the scope of the fraud problem, the full nature and extent of the fraud problem in Australia is not fully known. This is due, in large part, to the hidden nature of white-collar crimes such as fraud and to under-reporting of fraud in the private sector[36]. The federal Attorney-General's Department, in its report on *The Changing Nature of Fraud in Australia*, note that it is estimated that two-thirds of fraud offences which are committed in the private sector are not reported.[37]

---

33 For an explanation of how these costs were calculated see p3 of the report, op cit n 27.

34 AIC & PricewaterhouseCoopers, *Serious Fraud in Australia and New Zealand*, 2003, AIC Research and Public Policy Serious No 48, pp2-3; Minister for Justice and Customs, Senator the Hon Christopher Ellison in his *Media Release* "Serious Fraud in Australia and New Zealand", 27/3/03.

35 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*, p 3.

36 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, pp 10-11.

37 Australia, Attorney-General's Department, *The Changing Nature of Fraud in Australia*, 2000, p 3. They note that the reasons for under-reporting include: detriment to business (ie in

Factors which influence fraud

According to a recent report by the Commonwealth Attorney-General's Department, there are many factors which influence fraud. These include: globalisation; technological influences and advances such as the rise of the internet and e-commerce and the increased scope of such influences for identity fraud; economic influences such as corporate governance and outsourcing; as well as social influences (for example increasing workforce mobility).[38]

Cost of fraud

Estimates of the cost of fraud vary. As noted in the introduction, a figure often cited is $3.5 billion dollars, although the cost of identity fraud alone has been estimated at almost the same amount. Recent reports cite the cost as being closer to $5 billion.[39] This represents almost a third of the total estimated cost of crime in Australia (which is put at $19 billion).[40]

3. IDENTITY FRAUD

A distinction can be drawn between identity fraud and identity theft. Identity fraud refers to the creation and use of false identification or identities whereas identity theft refers to the theft of a person's existing identity (stealing someone's identity or impersonating an individual).[41] Identity fraud is an expression that is often used to encompass both types of fraud in question.

Identity fraud has been described as a tool which is used to facilitate some other criminal act.[42] As noted by Dr Brandi, a forensics expert for the Australian Federal Police, identity

---

terms of reputation and custom); dissatisfaction with the outcomes of previous criminal proceedings; lack of awareness; and a preference to take action in an attempt to recover losses without laying of criminal charges.

38 Australia, Attorney-General's Department, *The Changing Nature of Fraud in Australia*, 2000.

39 op cit, n 34.

40 AIC, "Crime costs Australia almost $32 billion each year", *Media Release*, 9/4/03. Note the cost of crime is put at $19 billion while the cost of dealing with crime (eg policing and prisons) is close to $13 billion (a total of $32 billion).

41 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002. Identity theft has also been described as an "impersonation of a specific individual": LoPucki Lynn M, "Human Identification Theory and the Identity Theft Problem, *Texas Law Review*, 80 no 1, 2001, p 90.

42 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, p 2.

fraud "has become an enabler for many other crimes...A false or stolen driver's licence is not usually used to drive a car but to provide identity for illegal immigrants, tax evasion or money laundering."[43] An example of a type of criminal act is given below.[44]

The problem of identity fraud has been highlighted by events both before and in the aftermath of the September 11 attacks on the World Trade Centre in New York[45]. In the former case false documents (false affidavits and residency certifications) were used to facilitate access to official identification papers. The official papers then allowed the terrorists to board the planes. In the latter, there were many cases where individuals adopted the identity of victims of the tower attacks, and relied on the goodwill of financial institutions and other organisations to obtain banking accounts and identification claiming that their paperwork had been destroyed in the towers.[46]

It has been said of identity fraud that it "is one of the fastest growing, and insidious crime problems in the world today. Its myriad forms and use in facilitating a number of crimes poses unique and unprecedented challenges that require not only greater planning, coordination, and cooperation within and among government agencies, but with those across national borders as well."[47]

The problem of identity fraud has reached such significant proportions that the US Department of Treasury convened a *National Summit on Identity Theft* for the first time on 15 March 2000.[48]

Factors which influence identity fraud

As noted above, there are many factors which influence fraud in general. In relation to identity fraud specifically, technology is a key factor which has influenced the rise in identity fraud. This is in two key respects: in terms of weakening the integrity of identification (the ability to forge documents for example)[49]; and the widespread collection and dissemination of data (in electronic form) on individuals by private sector and other

---

43 Dearne K, "ID card would 'curb fraud'", *Australian IT*, 13/11/02. Article available at http://australianit.news.com.au; Bajkowski J, "Identity fraud under surveillance", *Computerworld*, Vol 25A No 18, 4/11/02, p 1.

44 However, there are many other types of criminal acts which are facilitated by identity fraud.

45 These have been outlined by Pontell in his paper, op cit n 42, at pp2-3.

46 AIC, "Identity Fraud", *AIC Newsletter*, Summer/Autumn 2002, no 17, p 1.

47 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, p 3.

48 Hemphill T A, "Identity Theft: A Cost of Business?", *Business and Society Review*, 106 no 1, Spring 2001, p 61.

49 Australia, Attorney-General's Department, *The Changing Nature of Fraud in Australia*, 2000, p 10.

organisations which provides opportunities for easier access to personal information.[50]

Who commits identity fraud?

It has been said that identity fraud is "employed by individuals, organised crime groups and terrorists". Also, that "It generally involves a person falsely representing him or herself as either another person or a fictitious person. It may also take the form of a person fraudulently representing themselves through the misrepresentation of crucial facts regarding their own identity."[51]

How is it perpetrated?

There are many ways in which personal information is 'manufactured' or obtained. These include the use of high-tech means (such as the use of technology to either create false identification or access personal information) as well as non-technological means (such as sifting through rubbish bins for bank statements and other information, or looking over someone's shoulder as they use an ATM).

Hemphill states: "These misrepresentations of same, stolen or fictitious identities are made possible by either obtaining (through theft or fraud) documents and/or personal data of another individual, or by the production of false documents themselves...By taking advantage of weak or ineffective identification and authentication systems, criminals have victimised consumers, credit card companies, government agencies, businesses, and entire nations."[52]

In addition to taking advantage of weak or ineffective ID systems, information is also obtained by stealing mail, looking over someone's shoulder whilst they are using a phone, computer or ATM ("shoulder-surfing"), or by scanning credit cards via an electronic device such as at a point of sale ("skimming").[53]

Magnitude of identity fraud

The Federal House of Representatives Standing Committee on Economics, Finance and Public Administration, in their report on a review of the ANAO Audit Report on the management of tax file numbers,[54] state that indications of the extent of the problem of identity fraud include the following:

- 'the estimate would be that approximately 25 per cent of reported frauds to the AFP

---

50 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502. Mike Hatch is the Minnesota Attorney General. p 12 of internet download.

51 ibid.

52 ibid.

53 Rann M, "Crackdown on Identity Theft", *Media Release*, 25/2/03.

54 Australia, Parliament, House of Representatives Standing Committee on Economics, Finance and Public Administration, *Numbers on the Run: Review of the ANAO Audit Report No 37, 1989-99 on the management of Tax File Numbers*, Canberra, 2000, Section 6 "Identity fraud and Proof of Identity processes".

involve the assumption of false identities';
- Federal Agent Williamson observed that 'when I was a fraud investigator, most fraud offenders had multiple identities available to them, whether they were used or otherwise';
- that 'identity kits' consisting of a set of fabricated documents for a false identity are 'increasing in availability, particularly due to the ability of modern technology to generate forged documents of very high quality';
- 'that identity documents of various types are available for the payment of money – either forged documents or genuine documents which have been stolen and otherwise dealt with', including via the Internet;
- that in a pilot study conducted by Westpac and the NSW Registry of Births, Deaths and Marriages of a Certificate Validation Service, in 'the particular instances where a birth certificate was tabled to the bank as part of the identification documentation, some 13 per cent were found to be false';
- Centrelink detected 'about $12 million worth of fraud from identity' in 1999; and
- the National Crime Authority's (NCA) concern about the ease 'with which false identities may be established and used to facilitate organised criminal activity'.[55]

The Committee noted that various estimates of the magnitude of the problem (in terms of cost), and anecdotal evidence, suggested identity fraud was increasing. However, the Committee was still "concerned at the lack of figures available on the extent and cost of identity fraud".[56]

The Committee recommended, "That the Commonwealth Government work with other levels of government and industry to develop national statistics on the extent and cost of identity fraud in Australia."

Examples of identity fraud and theft

The types of fraudulent acts that can be perpetrated with false or stolen identities are wide-ranging.

Obtaining bank loans under false identities: Recently in NSW it has been reported that illegal finance brokers are manufacturing false identities for customers. This is so that the customers are able to obtain bank loans of up to $50,000 in value, which will never be repaid.[57] The article notes:

> For a $500 upfront charge, the brokers create the new identity along with documentation required to satisfy the 100-point identification system banks use for granting unsecured loans.
> In two days they can produce fake drivers' licences, council rates notices, Medicare cards, employers' references, credit cards and bank statements. ...

55 ibid, p 67, citing various transcripts of evidence.

56 ibid, p 68.

57 "Forging an new 'industry' of fraudulent bank loans", *The Daily Telegraph*, 24/2/03.

> What the brokers ask for in return is a cut of the loan once it is granted – usually half.

The report notes that according to police "...the fraudulent loan industry is flourishing across Sydney, mainly in the west but also in the east and the city." According to the media report "One senior police source, who did not wish to be named, said there were now 'dozens' operating from homes". The source stated "It's a thriving suburban industry...you just need a little bit of nous and access to the documents."

According to the article, the head of the NSW Fraud Squad, Detective Superintendent Megan McGowan, stated that due to technological advances (particularly the prevalence of home office technology) forging documents was much easier and that as the 100-points system was developed prior to such technological changes, it now required an overhaul. She stated "A number of documents permissible under the 100 points system are so easy to duplicate they should be excluded". She also stated that in order to obtain 100 points there should be at least one piece of high-value photographic ID.[58]

'Skimming' credit and other cards: According to a recent media report, a major bank's ATMs were targeted in a skimming fraud which robbed 100 cardholders of an amount of more that $300,000.[59] Skimming refers to the process whereby an electronic device is used to obtain details of card holders.

Fraudulent use of credit cards: The Australian Consumers' Association (ACA)[60] alerted consumers to a credit card scam being conducted over the holiday season (in December 2001) where discarded receipts were being used to fraudulently purchase goods over the internet and phone. According to the article, police were investigating reports that the receipts were taken from rubbish bins in shopping centres. The ACA recommended that consumers take care when disposing of receipts.

Another recent article by the ACA reports that consumers should be cautious in checking credit card statements to report unauthorised transactions as otherwise banks may refuse refunds in such cases. They use the example of a couple in the NT who went travelling for 15 months and did not check their statements during this time. According to the article their card had been fraudulently debited almost $7000 during this period.[61]

There have been many other examples reported in the media.[62]

---

58 ibid.

59 Lebihan R, "Police taskforce targets e-fraud', *The Australian Financial Review*, 2/4/03, p 52.

60 ACA, *Alerts: Scams, New credit card scam,* December 2001. Available at http://www.choice.com.au under articles.

61 ACA, *Money: Tips & Traps, Credit cards: No refund for fraud*, July 2002. Available at http://www.choice.com.au under articles.

62 See for example the following articles: "Alert on ATM scam as secret scanner seized", *The Sun-Herald*, 8/12/02; "Credit card fraud booming: Service stations hub of scam", *The Daily*

US experience

Identity theft has also been a growing problem in the US.[63] One commentator stated that between 500,000 and 700,000 people in the US would have their identity stolen in 2001 and that the cost to consumers of this problem is nearly $1 billion per year[64]. The cost to individual victims of identity theft was an average of $18,000 in unauthorised charges.[65]

A recent media report also notes that up to 700,000 people in the US may be victimised each year by identity thieves. The report notes that in 2002, complaints about identity fraud nearly doubled. The FTC stated that 43% of 380,000 complaints involved identity theft.[66]

Commentators in the US and elsewhere have highlighted a link between the erosion of privacy and a corresponding increase in identity fraud. Mike Hatch, Minnesota Attorney General, has said that, "Identity theft is directly related to the erosion of privacy"[67] and that "On average, companies trade and transfer personal information about every US citizen every five seconds".[68]

Hatch also notes, in the US context, that:

> As personally-identifying information has become freely available, the rate of identity theft has increased...The total number of inquiries...[to the Fraud Victim Assistance

---

Telegraph, 27/11/02; "Banks given a lesson on fraud", *Australian IT*, 27/11/02; "Card sharks stalk ATMs: High-tech crims log on to our cash, *The Sun-Herald*, 17/11/02; "Gamblers in red turn to white-collar crime", *The Sydney Morning Herald*, 3/10/02; "300,000 missing mail fraud", *The Daily Telegraph*, 11/7/02; "Crooks rip off millions in dud pokie cheques", *Sydney Morning Herald*, 13/5/02; "Fake licences seized in raid", *The Sunday Telegraph*, 12/5/02; "Online action fraud alert", *The Daily Telegraph*, 12/3/02; "Shopping cash 'free' at Coles", *The Daily Telegraph*, 19/1/02.

63 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502.

64 According to LoPucki, the full magnitude of the problem in the US is based on estimates which "seem to be little more than guesses" due to the fact that there are no clear definitions and minimal data is collected. As such she states that the best estimates put the number of victims at more than 100,000 per year with a cost in excess of $2 billion per year: LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001, p 89.

65 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502. (p 13 of *Wilsons* full text download)

66 Ho D, "ID theft tops US fraud list", *Australian IT*, 23/1/02.

67 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502.

68 ibid, Wilsons (download) p 1.

> Department]...has...increased from 35,235 in 1992 to 522,922 in 1997, and yet, the free-flow of personal information continues virtually unchecked.

According to Hatch, the rise in identity fraud can be linked to technological advances which have led to the erosion of privacy: "Over the past ten years, commercial interests have collected massive amounts of information about individuals which is used readily to encroach on consumer privacy. The wide dissemination of such information and purchasing habits has harmed consumers by creating an environment susceptible to identity theft and unauthorized charges."[69]

Hatch argues: "The privacy debate should properly focus on the use of information beyond the legitimate purposes for which it was initially collected or disclosed – the so-called secondary use of information...[such as]...the harm caused when commercial entities share information with third party telemarketers or for marketing an affiliate's unrelated goods and services."[70]

Examples of how identity fraud is perpetrated

According to Hatch, a common way in which perpetrators commit identity theft is "...by opening a credit card account using their victim's name, date of birth, or Social Security number. They then use that credit card to rack-up charges for which they never pay the bill." Identity thieves can also "...open checking accounts and write bad checks, or establish cellular phone service, in the victim's name with no intention of paying the service fees." He notes that in such cases "...the delinquent charges are recorded on the victim's credit report...individual victims of identity theft spend an average of two or more years attempting to fix their credit report and restore their credit rating. [71]

Hemphill similarly describes how identity theft typically occurs:[72]

> In the scheme most commonly referred to as identity theft...the thief opens a credit account in the name of the victim. That account may be a credit-card account, an account for telephone or utility service, a lease of an apartment, or some similar credit extension. The thief obtains money, goods, or services, charges

---

69 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502, p 12 of internet download.

70 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502. Therefore the strengthening of privacy protection can have positive outcomes in terms of preventing identity fraud.

71 Hatch M, "The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century", *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457-1502.

72 Hemphill T A, "Identity Theft: A Cost of Business?", *Business and Society Review*, 106 no 1, Spring 2001, pp51-63.

> them to the account, and then disappears. This type of identity theft has two victims. First, the firm that extends credit...will lose the amount extended. Second, the person whose name is used will be blamed for the fraud.

LoPucki discusses what happens after such an event occurs:

> Defrauded creditors have both legal and practical means for dealing with the problem. They are likely to employ such means as are cost effective, and pass the remaining costs on to their other customers...impersonated victims have neither legal nor practical means for dealing with the problem.[73]

In terms of the victims of identity theft:

> Although the impersonated victim is not involved in the fraudulent credit transactions perpetrated by the identity thief and suffers no direct loss from those transactions, the victim usually suffers from various secondary effects. Thinking that it extended credit to the victim, the defrauded creditor initiates collection against the victim. The action may include phone calls, written demands for payment, refusal to extend future credit, legal action, and perhaps most importantly, credit reporting. This often destroys the victim's ability to obtain credit from any source. In some cases, it may render the victim unemployable or even land the victim in jail.

4. CRIME STATISTICS

It should be noted from the outset that crime statistics on fraud do not provide a full picture as to the level of fraud that has been committed in the community. This is in large part due to, as noted earlier, the reluctance of organisations to report fraudulent activity to the police (particularly in cases where the fraud has been perpetrated by individuals within an organisation) and the overall hidden nature of white-collar crime such as fraud.

Federal

According to the AIC, approximately one-quarter of incidents involving fraud reported to the Australian Federal Police involve "the assumption of false identities".[74]

NSW

The latest *New South Wales Recorded Crime Statistics 2002* collated by the NSW Bureau of Crimes Statistics and Research (BOCSAR) does not show any significant trend for fraud

---

73 LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001, p 91.

74 AIC, "Identity Fraud", *Australian Institute of Criminology Newsletter*, Summer/Autumn 2002, no 17, p 3. The Australian Bureau of Statistics in their statistics on recorded crime do not include the category of fraud, so no information is available (nationally) from this source.

offences for the Period January 2001 to December 2002. By comparison, however, the *New South Wales Recorded Crime Statistics 2001* show that there was a significant upward trend from January 2000 to December 2001 (2 years) of the number of recorded criminal incidents[75] for fraud – up by 16.3%. The annual rate in NSW for 2000 was 427.2 incidents per 100,000 population. The annual rate in NSW for 2001 was 510.2 incidents per 100,000 population[76]. In 2002 the annual rate in NSW was 519.7 per 100,000 population.

The percentage change in recorded crime for fraud for the period January 1999 to December 2000 showed no significant trend.

The BOCSAR 2001 and 2002 reports show that there has been an increase in the recorded criminal incidents for fraud over the 4 years from 1999 to 2002 – a slight increase from 1999 to 2000, a significant increase from 2000 to 2001 and a slight increase from 2001 to 2002.

For further detail on crime statistics see Appendix A.

5. LEGISLATIVE AND OTHER RESPONSES

Responses to fraud can be varied. There can be, for examples, calls for tighter prevention measures, or the integrity of identification forms to be strengthened (the documents or cards themselves, eg licenses etc), or for privacy measures to be strengthened (so as to limit the amount of personal information that can be accessed, swapped, sold etc), or to increase criminal penalties for fraud or the utilisation of partnerships (such as public/private sector partnerships). Overall, a multi-faceted approach, with a focus on prevention, has been cited as the key to addressing fraud.

The Australian Institute of Criminology (AIC) divides the systematic responses to fraud into: corporate governance; private sector; and public sector initiatives. There can be considerable overlap between the three as well as the use of public/private sector partnerships.

In terms of legal responses to fraud, the AIC divides this into several areas: fraud reporting; investigation and policing; public/private sector partnerships; prosecution policies; trans-jurisdictional problems; court processes; legal problems and sentencing.[77]

How should fraud be addressed?

The AIC has stated that policies and practices are needed to: "reduce the supply of

---

75 A recorded criminal incident is defined by BOSCAR as an "activity detected by or reported to police which: involved the same offender(s); involved the same victim(s); occurred at the one location; occurred during one uninterrupted period of time; falls into one offence category; falls into one incident type (for example, 'actual', 'attempted', 'conspiracy')." p vi.

76 BOCSAR, *New South Wales Recorded Crime Statistics 2001,* 2002, pp 4, 12.

77 Graycar A, Director AIC, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*.

motivated offenders; protect and educate the suitable targets; and limit opportunities by making the crime more difficult to commit." It states that ways in which this can be done are:

- ...[in]...reducing the supply of motivated offenders, judicial punishments also play a role. Prison, which has few redeeming features, probably works better as a deterrent for fraud offenders than for many others. Similarly, confiscating a fraudster's home or car and requiring ill-gotten gains to be repaid over a lifetime are appropriate sanctions for white collar offenders.
- ...protecting and educating the targets of fraud is a crucial part of the prevention equation. It involves a knowledgeable and informed public able to identify an offer which appears "too good to be true"...
- Limiting opportunities by making the crime more difficult to commit brings in the other side of the prevention equation, corporate governance and professional regulatory procedures. The technologies of crime prevention are also of fundamental importance here.

With respect to prevention, the AIC note that "...the increasing recognition that the best line of defence against fraud is self-help has moved many private sector organisations to introduce and to improve fraud control systems." The AIC notes that failure to introduce such systems "...may, in the future, result in corporations being subjected to civil and criminal penalties, not to mention bad publicity, poor profitability, and disruption to their operations."[78]

The Federal Attorney-General's Department have stated that there are many implications and challenges for law enforcement agencies in grappling with fraud, for example, the collation of better data, the finite amount of law enforcement resources available coupled with the high costs in investigating fraud, and the limited role of law enforcement agencies with respect to prevention[79]. They note:

> The mechanisms, processes and strategies used for prevention, detection, investigation and prosecution of fraud will need to become more sophisticated and comprehensive, if they are to deal not only with the human aspects of fraud but with the highly technical nature of the systems being utilised to facilitate fraud. Increased inter-jurisdictional and, particularly, international cooperation will be vital to ensure that these processes can work efficiently. This cooperation will have to include some degree of regulatory or legislative consistency. Increased cooperation and

78 Graycar A, Director Australian Institute of Criminology, "Fraud Prevention and Control in Australia", *Paper presented at the Conference on Fraud Prevention and Control on 24-25 August 2000*. (p 5 of 12 internet download)

79 Given that it is up to individual organisations to take measures to improve prevention.

> information sharing within the private sector and between the private sector and law enforcement agencies would also facilitate prevention, detection and investigation of fraud.[80]

They conclude that:

> Solutions to the problems lie in increased awareness of the changing risks...; in prevention, including the widespread use of effective electronic security and identity verification systems; and in international cooperation in regulation, information sharing and enforcement.[81]

A recent paper on identity fraud emphasised that "Trying to deal with identity fraud through criminalization alone, cannot serve as an effective means of control. The agencies that might best foster this do not involve law enforcement, but the documentation and authentication of identity itself."[82]

NSW responses

Legislation

Crimes Amendment (Computer Offences) Act 2001 (NSW)
This Act creates new offences for the commission of computer-based crime, such as hacking, circulating viruses, and the facilitation of identity theft offences. The Act was developed in accordance with model provisions that are contained in the report of the Model Criminal Code Officers Committee (of the national Standing Committees of Attorneys-General). The Act facilitates a move "towards a uniform approach to computer offences, both nationally and internationally."[83]

Increasing penalties – According to a recent newspaper article the former NSW Police Minister, Michael Costa, stated "New technology means criminals are becoming more sophisticated and the law must keep pace with technology".[84] He indicated that proposed new laws would deal with trafficking in credit card data and in the manufacture, possession or trafficking of devices used to forge credit cards.

---

80 Australia, Attorney-General's Department, Office of Strategic Crime Assessments, *The Changing Nature of Fraud in Australia*, 2000, p 14.

81 ibid p 17.

82 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, p 14.

83 Mr Debus MP, 2nd reading speech, NSW*PD*, 4/4/01, p 13167.

84 "Jail for Skimmers", *The Sunday Telegraph*, 16/2/03, p 29.

Strengthening integrity of identification - Other measures have been introduced which have been suggested as being helpful in combating fraud. These measures generally relate to strengthening the integrity of identification.

For example, allowing drivers license photos to be stored, which the former Minister for Transport (Carl Scully) in 1999 stated would help prevent fraud:

> Photo storage is vital to counter fraudulent applications for driver licences using another person's proof-of-identity documents. A replacement licence will not be issued unless the applicant matches the facial image stored in the system. This will significantly enhance the integrity of the licensing system in preventing fraudulent transactions. Preventing the use of fraudulently obtained identities will provide the community with considerable benefits in terms of the prevention of serious fraud and accountability of licensees, vehicle operators and owners.
>
> The types of fraud that will be prevented include credit or financial institution fraud, social security fraud, rebirthing of stolen vehicles, under-age purchasing of alcohol and tobacco, or entering into licensed premises. So far as this concerns the primary purpose of the licence - driver management - the bill enhances the integrity of the licence record and aims to frustrate those who would evade their responsibilities. While meeting community expectations on the security of photo licences, photo storage will also lead to better customer service. The Roads and Traffic Authority will be able to positively identify the genuineness of a customer efficiently without imposing series of checking procedures that could be seen by some customers as unduly onerous and time-consuming.[85]

The relevant amending Act is the *Road Transport (Driver Licensing) Amendment Act 1999*[86] which amended the *Road Transport (Driver Licensing) Act 1998* (NSW) so as to set out the circumstances in which the RTA could retain and use photographs of people.

In addition, the NSW Roads and Traffic Authority have trialled a system whereby they have had online access to the birth records (from the NSW Registry of Birth, Deaths and Marriages) so as to verify customer identity claims.[87] This verification process has now been formalised in NSW.[88]

---

85 Hon Carl Scully MP, *NSWPD*, 27/10/99, p 2095.

86 Passed in 1999, assented to 24.11.1999 and subsequently repealed by the *Statute Law (Miscellaneous Provisions Act 2001* No 56.

87 Australia, Attorney-General's Department, *The Changing Nature of Fraud in Australia*, 2000, p 10.

88 Chapman A and Smith R, "Controlling Financial Services Fraud", *trends & issues in crime and criminal justice*, February 2001, p 5.

Federal

According to a recent press release by the federal Minister for Justice and Customs, Senator the Hon Christopher Ellison, there have been many federal developments in terms of developing fraud prevention strategies. He stated that work was being done by the National Fraud Desk at the Australian Crime Commission "in coordinating intelligence and strategic information on fraud and its prevention". The federal Government also introduced last year revised Fraud Control Guidelines assisting "the Commonwealth in gathering quantitative data to gauge the amount of fraud being perpetrated against its own agencies."[89]

In addition, a national scheme linking driver's licence databases from all states and territories is under way.[90]

South Australia

The Premier of South Australia, Mike Rann, recently announced that the SA government would introduce legislation to make identity theft a criminal offence. He stated: "We're the first in Australia to launch a crackdown on people using someone else's personal information with the intention of committing a crime". He noted that identity theft (a crime of the "new millennium") was a significant enabler of other crimes such as: terrorist activities; fraudulently establishing credit; running up debts; or taking over existing financial accounts. Identity theft poses a significant problem because it is only when stolen or fake identification is used to commit a crime that police can act to prosecute offenders.

According to a media release by the Premier, the SA Government is proposing to make it an offence to:

- Knowingly assume a false or fictitious identity and use that identity to commit a serious offence;
- Knowingly produce, possess or sell (without lawful authority) personal identification information intending to commit a serious offence;
- To produce, possess or sell document-making equipment intending to produce or obtain unauthorised means of personal-identification information.[91]

The SA Government is intending to consult with business and law-enforcement agencies before introducing legislation this year.

Possible solutions to the problem of identity fraud

Various possible solutions to the problem of identity fraud have been mooted. Many of these policy and other proposed solutions embrace a greater use of technological tools to combat the problem of identity fraud – such as the use of biometric technology to identify people (for example via scans of unique body parts such as the iris, finger, hand etc); a

---

89 Hon Christopher Ellison, Senator, federal Minister for Justice and Customs, "Serious Fraud in Australia and New Zealand", *Media Release*, 27/3/03.

90 Chapman A and Smith R, "Controlling Financial Services Fraud", *trends & issues in crime and criminal justice*, February 2001, p 5.

91 Ibid.

national biometric card; and the use of a centralised identity database to capture information.

Use of biometric technologies

On the issue of fraud, and identity fraud in particular, the head of banking and property for Macquarie Bank, in conjunction with the release of a consumer guide to avoiding identity theft, reportedly stated that the use of biometric technologies would be an inevitable outcome of identity theft.[92]

In the same report it was noted that iris-scanning technology was already in use in ATMs in Britain and America and would become commonplace in Australia within the next five years.[93]

A national biometric ID card

There have also been suggestions that a National biometric ID card would help curb identity theft.[94] It was reported that Australian Federal Police forensics expert James Brandi stated that a national card "would solve a lot of problems". He stated "As criminal activity patterns shift to ID theft the impact is worse for individuals" and "Your credit rating can be destroyed within a matter of hours".

Whether or not a move to national ID card would help fraud or simply erode privacy further is debatable. As noted earlier the rise in fraud such as identity fraud has been directly linked to the erosion of people's privacy due to technologies that allow companies and others to access varying degrees of personal information. Indeed attempts at introducing a national card have been strongly resisted in the past due to public concern over privacy[95].

There have been many views expressed in regard to the use of biometric technology in this regard, particularly with respect to the ramifications for individual privacy:

A report by the federal Attorney-General's Department has stated:

> The use of biometric identification, such as digital fingerprints, coupled with online access to other confirmatory information, such as digital photographs, also has the potential to improve the security of identification authentication methods. None of these methods will provide absolute proof of identity, however. These

---

92 "Police, help, they took my identity", *Sydney Morning Herald*, 28/2/03.

93 According to John Grimes of the company Argus Solutions - which deals with iris scanning technology.

94 Dearne K, "ID card would 'curb fraud'", *Australian IT*, 13/11/02. Article available at http://australianit.news.com.au. Note: as to whether biometric technology is currently viable or accurate see the following article: Messmer E, "Is biometrics ready to bust out?", *Computerworld*, Vol 25A No 18, 4/11/02, pp22-23.

95 Bennett J, Member of the National Crime Authority (NCA), *Identity Fraud: Getting Inside the Criminal Mind*, 4 May 2001.

> technological developments would need to satisfy privacy requirements before they could be brought into wide-spread use.[96]

The head of the NSW Fraud Squad, Megan McGowan, was reported as raising concerns about the technology, saying: "Once someone acquires your fingerprint and finds a way to use it, what do you do? You can't ask the bank to issue a new finger."[97]

Whilst many commentators advocate the use of technologies to remedy the problem of identity fraud, such technologies do have limitations and are not infallible. Pontell notes that technological solutions cannot, alone, provide a solution to the problem of fraud:

> Professor Gary Marx, one of the world's leading authorities on surveillance, technology and social control mechanisms, points out that in complex settings in democratic societies, "relying primarily on technology to control human behavior has clear social and ethical limitations." Simply put, regardless of how ideal a technical control system may appear in the abstract, it is inevitably subject to the harsh realities of implementation and actual practice. ... As Marx notes, ..."Technical efforts to insure conformity may be hindered by conflicting goals, unintended consequences, displacement, lessened equity, complacency, neutralization, invalidity, escalation, system overload, a negative image of personal dignity and the danger of them means determining, or becoming the ends." All of these concerns need to be examined before implementing technological "solutions". Moreover, the lack of privacy concerns and awareness in various sectors of society as well as the careless use of personal information provide structural gaps in the social control of personal identity that criminals continue to exploit. As seen by the example of missing computers...[In the US, the Internal Revenue Service could not account for thousands of missing computers]..., the government may itself inadvertently contribute to the escalation of the same fraud it wishes to suppress.[98]

Pontell also discusses how technological control can be undermined or compromised by simple human interactions. He gives the example of a thief who was unable to break a sophisticated encryption code, but nonetheless was able to embezzle millions of dollars by having an affair with the individual who had the encryption codes.[99]

---

96 Australia, Attorney-General's Department, *The Changing Nature of Fraud in Australia*, 2000, pp10-11.

97 "Police, help, they took my identity", *Sydney Morning Herald*, 28/2/03.

98 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, p 15.

99 Ibid, citing Marx GT in "Technology and Social Control: The Search for the Illusive Silver

Use of Centralised Databases

The use of centralised databases, which are controlled by government agencies, has been raised as a possible solution to the problem of identity fraud. The method in which databases can be employed can differ, for example they can contain a register of victims of identity theft or can be used to authenticate the identity of all individuals.

For example, the US state of California enacted a law in 2001 establishing an identity theft database. Under the law, the state is required to keep a database of persons who have been victims of identity theft. Access is only granted to certain government agencies (such as criminal justice agencies) and victims. The purpose of the database is to provide a means for victims to prove that they have indeed been victims.[100]

Other types of databases could be established to authenticate all individuals. The use of such databases can raise many security and privacy concerns. Pontell notes that such "security and privacy issues associated with large government databases present major problems". He cites the example of legislation introduced in the United States Congress following the September 11 attacks to create a standardised identification system which would link existing information in state motor vehicle databases. This would lead to the creation of a standardised driver's license which would incorporate technological security features such as biometric identifiers (ie fingerprints).[101] The card would become in effect a national ID card. Whilst the proposed legislation was supported by the American Association of Motor Vehicle Administrators, serious privacy and security concerns were raised by others such as the National Academies of Science.

Other

Strengthening the authentication process in order to properly identify individuals

Other methods to combat or minimise identity fraud have been proposed, such as a more thorough process for investigating or authenticating the identity of customers prior to the provision of credit. Identification of consumers becomes more difficult when there are faceless transactions. As many transactions are now conducted over the phone and internet, and this has proved to be both popular and convenient, the potential for identity fraud has increased. Some methods of strengthening processes for authenticating the identity of customers may prove, however, to be unacceptable to consumers or financial institutions. For example, it has been said that, from the point of view of credit providers and credit reporting bureaus, this poses difficulties for such organisations as "these firms calculate that it is not cost efficient to engage in improving security practices...." [102] As Hemphill notes:

Bullet", *International Encyclopaedia of the Social and Behavioural Sciences*, 2001, p 1.

100 LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001, p 113. California Penal Code § 530.7(c) (Supp. 2001)

101 Pontell H, University of California, Irvine, "Pleased to meet you...won't you guess my name? Reducing identity fraud in the Australian Tax System", Paper presented at the Centre for Tax System Integrity, ANU, *Identity Fraud and Illegal Tobacco: An Absence of Integrity*, Sponsored by the Australian Taxation Office, 29 October 2002, p 16.

102 Hemphill T A, "Identity Theft: A Cost of Business?", *Business and Society Review*, 106 no

"After all, a certain amount of fraud is simply a cost of business, regardless of what economists refer to as the negative externality borne by the victimized consumer."[103]

From the point of view of consumers, this may lead to delays in processing transactions or the use of technologies which may prove unacceptable.[104]

US responses

As noted earlier, the Minnesota Attorney General, Mike Hatch, has argued that increasing levels of fraud (such as identity fraud) are undoubtedly linked to the erosion of privacy which has been brought about by increased technology.

In order to rectify this, he argues that:

> There is an immediate need to enact privacy laws governing the use of personal information such as bank and telephone records. This need is more acute as deregulation and technology have allowed institutions to merge, affiliate, and associate such that massive amounts of highly confidential information may be readily shared among them. Neither existing laws nor self-regulatory efforts are adequate to protect consumer privacy in the information age. The lack of protection undermines an individual's right to privacy and choice.[105]

LoPucki states that:

> Congress's first attempt to respond to the problem – the Identity Theft and Assumption Deterrence Act of 1998 – has had little effect. Several bills directed at identity theft are now pending in Congress and nearly all states have enacted their own legislation. But even the staunchest advocates of the proposed reforms admit that they will not solve the problem. Identity theft is out of control.[106]

LoPucki outlines several conventional approaches/solutions to the problem of identity theft,

---

1, Spring 2001, pp53.

103 Hemphill T A, "Identity Theft: A Cost of Business?", *Business and Society Review*, 106 no 1, Spring 2001, pp53. He further states that "With this enlightened approach to corporate responsibility, is it any wonder that retail credit issuers and the consumer credit reporting industry are under increased scrutiny by the media, consumer groups, and the federal government?"

104 The challenge appears to be to devise systems and processes which are cost-effective for organisations and which prevent unauthorised charges and withdrawals as well as which are acceptable for consumers. "Banks target credit card and net fraud", *The Australian Financial Review*, 20/3/03, p 25.

105 Hatch M, op cit n 69, pp 19-20.

106 LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001, p 90.

and then outlines, in her view, why such conventional approaches to curbing identity theft are inadequate. The conventional approaches are outlined as being:

- Keeping personal information secret
- Banning the use of social security numbers
- Requiring the use of more or better characteristics (ie requirement that at least 4 characteristics match), or use of biometric characteristics
- Improving the integrity of identifying documents
- Victim-assistance programs
- Making creditors and credit reporting agencies liable for misreporting on victims of identity theft
- California's identity-theft database[107]

As she believes that the above approaches cannot work, she provides an alternative proposal which in effect is a system which enables a creditor "who seeks to determine the identity of a credit applicant to contact the true owner of that identity for confirmation". That system involves the creation and use of a centralised database which would entail "...a website that contained contact information for participating consumers and a procedure by which the government agency in charge of the website would decide who was the true owner of each identity and therefore entitled to list the contact information for that identity".[108]

Responsibility resting with the private sector

One commentator has argued that the various measures introduced in the US, whilst welcome, would not solve the problem of identity theft fraud due to the fact that the primary responsibility for identity theft prevention rests in the private/business sector:

> While the efforts of federal and state governments to provide greater penalties, criminal enforcement, theft prevention, and victim remediation of identity theft are necessary and welcome, the primary institutional responsibility for identity theft prevention and victim remediation rests in the business sector. After all, business is the issuer of credit and provider of services and products that are the targets of the perpetrators of identity theft. [109]

For further information on different private sector views see Section 7 below.

---

107 LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001. See her article for further information on why she believes these approaches are inadequate.

108 LoPucki L, "Human Identification Theory and the Identity Theft Problem", *Texas Law Review*, 80 no 1, 2001, p 114. See her article for further information on this proposed system.

109 Hemphill T A, "Identity Theft: A Cost of Business?", *Business and Society Review*, 106 no 1 Spring 2001, p 57.

6. LAW ENFORCEMENT INITIATIVES

New South Wales Police

A new State Crime Command was established in the NSW Police in 2002.[110] It is comprised of 9 specialist investigative units (squads), which includes the Fraud Squad. The Fraud Squad is headed by Detective Superintendent Megan McGowan.

According to the *Fraud Prevention Guidelines*[111] the NSW response to fraud related crime includes the following[112]:

Local Area Commands (LACs)

- Responsible for the investigation of fraud offences which occur within their area
- Responsible for the investigation of serial fraud offences outside their area where the initial offence occurred within their area

Region Commands

- Responsible for the investigation of fraud offences that occur across Local Area Command boundaries within their Region.
- Responsible for the investigation of serial fraud offences that occur outside their Region where the initial offence occurred within their Region. [113]

In addition, the recently created Fraud Squad addresses fraud across the state.

According to a recent media report, the NSW Police are establishing a computer crime taskforce to protect consumers from electronic fraud. The report notes that Detective Superintendent Megan McGowan is most likely to head the taskforce. The article notes that: "American Express and the Commonwealth Bank of Australia are already on board, with the Australian Federal Police High Tech Crime Squad and NSW Crime Commission having expressed an interest in the group."

The aims of the taskforce include:

- the prevention of electronic crime against financial institutions; and
- to provide advice, training and high level expertise to businesses.[114]

---

110 It was announced in November 2002: "Shake-up of crime fighters starts with a name", *The Sydney Morning Herald*, 8/11/02, p 6.

111 Available from http://www.police.nsw.gov.au The publication is not dated.

112 This information is reproduced from the guidelines

113 For a review of the police response to fraud see the following report by the NSW Audit Office: NSW, Audit Office, *Performance Audit Report: NSW Police Service: police response to fraud*, 1998.

114 "Police taskforce targets e-fraud", *The Australian Financial Review*, 2/4/03, p 52.

The New South Wales Crime Commission

The New South Wales Crime Commission ('the Commission) was established in 1986 to combat illegal drug trafficking and organised and other crime in NSW.[115] Among other functions, the Commission is required to investigate matters relating to criminal activities referred to the Commission by the Management Committee, to assemble admissible evidence of relevant offences and to furnish that evidence to the Director of Public Prosecutions.[116] In its latest *Annual Report* for 2001/02 the NSW Crime Commission reports on the patterns or trends as well as the nature and scope of crime that has been observed during the year.[117] With respect to computer crime and identity fraud the Commission notes that statistics from Australia and the US indicate "there has been a significant increase in all types of computer crime"[118] and that such computer based crime covers a broad range of criminal activity which can include the use of computers to commit other crimes such as money laundering, fraud, and the creation of false identities.

The *Ebenezer* Reference into computer-based crime was referred to the Commission in December 2001. The Commission has established a joint task force with the NSW Police on this subject. The Commission notes that "to date, the task force has investigated a small number of hacking, fraud and extortion offences." The Commission further notes that it "has made submissions to the government seeking amendments to Commonwealth laws that would enable remote access to computers used by criminals and the interception of telecommunications for the purpose of investigating state-based computer offences."

With respect to identity fraud the Commission notes they have on several occasions during the reporting year seized "false passports, driver's licences and other identifier documents that had been created or amended using computers." Also that recently, "during the execution of a search warrant by officers from Crime Agencies, a computer-based machine that produces driver's licences, which had been stolen from the Roads and Traffic Authority, was recovered from the home of a known criminal."[119]

---

115 Under the *New South Wales Crime Commission Act 1985* (NSW)

116 The principal functions of the Commission are to: investigate matters relating to 'relevant criminal activity'; assemble admissible evidence for submission to the Director of Public Prosecution; review police inquiries; furnish reports relating to illegal drug trafficking and crime; disseminate investigatory, technological and analytical expertise; and make applications for the restraint and confiscation of property under the *Criminal Assets Recovery Act 1990* (NSW). The *Criminal Assets Recovery Act 1990* (NSW) provides for the confiscation of assets of those involved in serious crime related activity through civil proceedings in the Supreme Court and the Commission has primary responsibility for administering this legislation.

117 New South Wales Crime Commission, *Annual Report 2001/02*, p 20. This is a requirement under the *New South Wales Crime Commission Act 1985* (NSW)

118 New South Wales Crime Commission, *Annual Report 2001/02*, p 21.

119 New South Wales Crime Commission, *Annual Report 2001/02*, p 21. Note: this raises interesting questions about the security of RTA data, if the machines themselves cannot be physically (or otherwise) secured adequately.

With respect to identity fraud in general they note:

> Using modern technology, documents such as birth certificates, driver's licences, motor vehicle registration papers, credit cards and many other documents used to establish identity can be easily forged. Verification of the authenticity of these types of documents, when used for identification, remains a significant problem. Document issuing authorities have inconsistent responses to the problem.
>
> Through consultation with representatives of both public and private sector institutions and examination of fraud detection systems in the private sector, the Commission found that attempts to capture and exploit new and historical data in relation to detected fraud, detected fraudulent identities and known cases of identity theft are either non-existent or fragmented. Where such databases did exist, access was limited and information was often not shared because of volume or due to commercial sensitivities. There was no system to facilitate the dissemination of information regarding identity fraud within or between private and public sector institutions.[120]

In light of the above problems posed, the Commission recommended the establishment of an identity fraud database, which would record known false identities and any instances of identity theft. Law enforcement agencies and financial institutions would use the database.

The Commission notes that a six-month pilot Identity Fraud Register was established by the Australian Bureau of Criminal Intelligence (ABCI) to assist investigators. The database "registers fraudulent identities, stolen identities and known identity fraud offenders detected by a number of public sector agencies." The participants in the pilot include: state and territory police agencies; twelve Commonwealth and state government agencies; and some private sector financial institutions.

According to the Commission, due to the success of the program it was extended to 31 December 2002.

Australian Federal Police

The Australian Federal Police (AFP) in their report on high-tech crimes[121], discusses the role of law enforcement in tackling high-tech computer crime.

They state:

> Computer crime and associated activities will continue to receive a high level of attention from the AFP. We now have computer

120 New South Wales Crime Commission, *Annual Report 2001/02*, p 21.

121 Australia, Australian Federal Police, *fraud@internet.com.au: The role of the Australian Federal Police in the investigation of high-tech crimes*, March 2000.

> crime teams in Brisbane, Canberra, Melbourne, Perth and Sydney. The AFP's current Electronic Forensic Support Team in Canberra will be re-structured to create a central Computer Forensic Facility to service the increasing demand for forensic analysis from within the AFP, and from our law enforcement partners. This facility will be supported by state-of-the-art computer technology and draw on the services of specialist computer professionals who are otherwise engaged in research and development activities for the AFP.

Other measures by the AFP include:

- The AFP has a dedicated Intelligence Collection manager for computer crime to ensure a link between operational and strategic issues which relate to computer crime.
- The AFP is a member of the Inter-Departmental Committee for the Protection of the National Information Infrastructure and the associated Consultative Industry Forum.
- The AFP is also a member of the Research Group on the Law Enforcement Implications of Electronic Commerce.

The AFP notes, "through these forums, the AFP will seek closer consultation with both public and private sectors to address the issues we face with the Internet and the opportunities it brings for fraud."[122]

7. PRIVATE SECTOR VIEWS AND RESPONSES

Insurance Council of Australia

The insurance industry has also been targeting E-commerce crime. The Insurance Council of Australia (ICA) released the *E-Commerce Crime and Vandalism Defence* on 9 August 2001. This guide was developed by the ICA to "raise the awareness of electronic crime and help insurers identify potential risks and legal issues surrounding E-commerce crime and vandalism". Alan Mason, Executive Director of ICA, notes that "E-commerce crime costs the global community approximately $3 trillion dollars each year...and has the potential to cause much greater damage than other types of fraud because nearly all financial transactions are conducted electronically".[123]

The resource is designed to assist insurers in the prevention, detection and response to such crime.

According to the ICA some of the greatest E-commerce threats include: "computer hackers, poor implementation of security policies and a lack of employee awareness of risks".

---

122 Australia, Australian Federal Police, *fraud@internet.com.au: The role of the Australian Federal Police in the investigation of high-tech crimes*, March 2000.

123 ICA, "Insurance industry fight against e-commerce crime", *Media Release*, 9/8/01.

KPMG Fraud Survey 2002

KPMG in their *Fraud Survey 2002* (which was outlined in greater detail in section 2) made the following observations: "...it is of concern that over 60% of respondents still believe that their organisations do not have a problem and are reticent to plan or implement steps to address the issue of fraud." Indeed, according to their survey results, 60% of respondents had not established a fraud strategy, 75% had not conducted training on fraud prevention and detection, 48% had not taken steps to improve security measures and 52% had not conducted pre-employment screening.[124]

KPMG, in their executive summary, concluded that "...many organisations in Australia and New Zealand, including many that have suffered serious fraud loss, are yet to implement even the most fundamental fraud prevention measures – measures that are often simple and inexpensive, yet effective."[125]

The Australian Shareholders' Association

When discussing the results of the *Fraud Survey 2000* released by KPMG, the Australian Shareholders' Association (ASA) was critical of the lack of action of Australian businesses and enforcement agencies to deal with fraud.[126]

With respect to law enforcement agencies the ASA has stated: "More and more people are reporting fraud of this nature...[external fraud such as international criminals committing major fraud and leaving Australia with the proceeds]...but the law enforcement agencies can't keep up because they do not have the resources."

ASA note, however, that the "...real problem or rather the answer to it is encapsulated in the old saying that an ounce of prevention is worth a pound of cure."

In other words, the problem of fraud in general needs to be tackled primarily from a prevention angle. To this end the private sector has the most significant role to play. The ASA further state that "It is a real indictment of Australian management that elementary internal controls often appear to be lacking and that so many businesses have neither planned, nor implemented appropriate fraud control strategies."

Australian Banking Association

With respect to fraud, the Australian Banking Association (ABA) issued a media release on 29 August 2000 welcoming recommendations from the Federal Standing Committee on Economics and Public Administration on reducing and preventing identity fraud. The acting Chief Executive of the ABA stated:

> I am pleased to see the Committee's recommendation that the Commonwealth Government work with industry to develop

---

124 KPMG, *Fraud Survey 2002*, p 19.

125 KPMG, *Fraud Survey 2002*, p ii.

126 Australian Shareholders' Association, "2002 Fraud Survey", *Shareholder Opinion Items*, available at: http://www.asa.asn.au/Archive.asp?ArchiveID=173

> options for reducing and preventing identity fraud, including the investigation and development of this secure national electronic gateway.
> For example, a drivers licence or a birth certificate could be checked directly with the government agencies through the gateway by a financial service provider when the documents are presented by the customer. Trials already carried out in New South Wales have confirmed this approach can assist in reducing the prevalence of identity fraud.

The ABA states that it is "also seeking consistency of documents used to validate a person's identity across all States and Territories and the tightening up of processes used when issuing documents to make it harder for criminals to obtain false identities."

The acting Chief Executive of the ABA also noted that identity fraud is not just an issue for the financial sector, government and industry but is an issue for the community as a whole.

In terms of individual consumer protection, the ABA has written a *Fact Sheet* on Identity Fraud and how consumers can protect their financial identity.[127] It lists 8 steps that consumers can follow to protect their identity. These involve the consumer:

- contacting Baycorp Advantage (formerly known as Credit Advantage Limited (CAL) and Credit Reference Association Australia (CRAA)) to obtain their credit reference file (or possibly arrange for a monitoring service – which has a cost attached)
- checking financial statements carefully upon receipt
- shredding or tearing receipts (and other personal information) rather than disposing of them in a casual way
- contacting their financial institution if statements are more than a fortnight late, or checking with Australia Post to ensure their mail has not been redirected.
- protecting account information ie not writing down Personal Identification Numbers (PINs) or entering PINs in a discreet way
- not carrying birth certificates or other identification documents such as passports and Medicare cards unless needed on the day[128]
- storing identification documents as well as account information in a secure place.

The fact sheet also provides information about what people should do if they become a victim of identity fraud: urgently contact the financial institution; notify police; contact Credit Advantage of Australia to review personal credit file; and check with Australia Post to determine if anyone has requested unauthorised redirection of mail.

---

127 It is available on the internet at: http://www.bankers.asn.au/ABA/Online/default.asp?DeptID=4&SubDeptID=&ArticleID=313

128 This suggestion might have some practical limitation in that individuals often always carry their Medicare card, as they may not know when the need for it may arise.

Banks

A recent media article notes that many of Australia's big banks are in the process of commencing a campaign to increase security on both online transactions and physical credit purchases. According to the article, several banks stated that the use of biometric scanning technology, however, was unlikely in the near future.[129]

Baycorp Advantage (formerly known as CAL and CRAA)

Baycorp Advantage was formerly known as Credit Advantage Limited (CAL) and Credit Reference Association Australia (CRAA)[130]. It was originally established as a consumer credit reporting agency that provided a credit reference checking service for businesses on individual consumers, but has over time expanded its data collection service to include companies and businesses. According to their website they "are the largest custodian of credit-related information in Australia and New Zealand...[and]...collect data on the financial behaviors of more than 13 million individuals and one million companies in New Zealand, Australia and Asia. And, each day we report on the credit status of the 60,000 individuals and businesses on both sides of the Tasman that apply for credit."[131]

Not only does the organisation provide information about credit behaviour but also, according to their website, offers other services such as database marketing and data mining services.[132]

Examples of the type of personal information stored on their database[133] are listed on the website. This includes personal information as well as detailed information about an individual's past credit behaviour. The information includes:

- name
- date of birth

---

129 "Banks target credit card and net fraud", *The Australian Financial Review*, 20/3/03, p 25.

130 The information below is taken from the Baycorp Advantage website at: http://www.baycorpadvantage.com.au. The website notes that "Baycorp Advantage unites two of Australasia's most important business support companies: Baycorp, the leading information solutions provider in New Zealand; and Data Advantage, the leading supplier of credit and marketing-related decision support services, data and software in the Asia-Pacific region."

131 See: http://www.mycreditfile.com.au to view the organisation profile. Note: There are other credit reporting agencies also operating in Australia.

132 The website states: "Once you have selected your customers, you can maximise their potential value by proactively managing the relationship. We have developed database marketing and data mining services, credit administration software, plus powerful behavioural and value assessment models, which allow you to understand and manage your customers current and future profitability."

133 The website puts it in somewhat more glossier terms: "Before you commit to a financial relationship with a potential customer, we can provide you with timely business information and detailed analysis about their past credit behaviour. That knowledge, along with our sophisticated software systems, will enable you to make quick, highly-informed credit and value based decisions from which to build a profitable customer base."

- drivers licence number
- current address
- previous address
- employment details (eg last known employer)
- other names by which a person is known (if any)
- credit applications and inquiries made over the past 5 years – type of credit applied for, with whom, and amount applied for
- overdue accounts listed against a consumers name (defaults)
- bankruptcy information
- judgments
- other public information such directorships or proprietorships

Many businesses and organisations use credit-reporting services. The way information is built up on such a database is through inquiries. For example, every time a financial, or other, organisation checks the credit history of a potential customer (before approving an application for credit) the information from that organisation about that application for credit is added on to an individual's file (if one exists) or a new file is created (if one does not exist). Other information is also added from other sources which are on the public record (eg judgment and writ/summons information from courts around Australia, bankruptcy information from ITSA and directorship or proprietorship information from ASIC).

Adverse information remains on file for five years and serious credit infringement such as bankruptcy remains on file for seven years.

Whilst financial organisations are a significant user of such a service, many other types of business and organisations also use them eg: telecommunications companies, electricity and gas companies, and retailers.

Baycorp Advantage lists information on their website about what an individual should do to both protect themselves from credit fraud and if they become a victim of credit fraud – they note that the most common form of credit fraud is identity theft. The self-protection measures listed are very similar to those outlined by the ABA above. They recommend that consumers check what is on their credit file and also that they make an application to have their credit file monitored so that they receive notification every time a credit application is made using the consumer's personal details.[134]

On the issue of identity theft, Baycorp Advantage has issued a media release recently announcing the establishment of a website www.mycreditfile.com.au to assist consumers in understanding identity fraud and how to protect their credit information and reputation.

The General Manager of Business Information Services, Ms Jane Wilson, highlighted that prevention is the key with respect to identity fraud as "taking action after a crime has been

---

134 Note: the monitoring service comes at a cost of $29.95 (as listed on the website - accessed on 10 March 2002).

committed is difficult, costly and often impractical" and further that "Personal reputations are often very hard to repair and offenders are frequently impossible to find." [135]

The way in which identity theft usually occurs, according to Ms Wilson is "where the thief obtains someone's identity details through lost or stolen wallets, credit cards, drivers' licences or stolen mail, and uses these to obtain a false identity and then secure credit for themselves." She notes "this leaves the victim with the potential liability for the debt and difficulties in obtaining future credit."

Australian Consumers' Association

The Australian Consumers' Association (ACA), in a *Media Release*[136] on identity fraud, discusses how consumers are more exposed today due to the increasing levels of electronic commerce. The way in which consumers engage with financial organisations and others has changed significantly as a result of the use of emerging technologies. As a consequence self-identification has become problematic. The Senior Policy Officer, IT and Communications, at ACA noted:

> Questions arise such as:
>
> - How does the telephone operator know it is really you adjusting your credit limit?
> - How does the web site operator know you are really authorised to use that credit card number?
> - How does the consumer prove it was a Trojan-horse program that dialled that high-cost porn site, and not them or someone else in the household?

He stated that business is reluctant to shoulder responsibility for this emerging problem:

> In such a new area, business is anxious to cast off the shackles of the past, and shift as much risk as possible onto consumers, by a judicious mix of technology and contract.

He discusses some of the problems with using a single highly authenticated identity, and says that the focus should be on information security:

> Many technologists favour a single robust identity for an individual. Once a single highly authenticated identity is seen as desirable, then the pressure is on to use it for as many purposes as possible. This is where many of the consumer issues and problems arise. We regard it as naive and dangerous to assume that a single authentic identity is necessary or even desirable for most consumers in society. It is also dangerous to confuse authentication with information security.

In particular, he expressed concerns with the increasing interest in biometric identification

---

135 Baycorp Advantage, "Rise in Identity Theft", *Media Release*, 23/1/03.

136 Australian Consumers Association, "Consumers' interests at risk as identity rules tighten", *Media Release*, 5/11/01.

(eg iris scans, fingerprint, face or voice recognition) by business:

> We are concerned about increasing interest of business in biometric identification...as well as using computers to monitor consumer behaviour. At the very least their usage must be disclosed and the consumer given the option to opt-out.

In the use of such identification technology, he states that businesses should be diligent in explaining the risks associated with its use. However, he notes that this is "not a substitute for: reducing those risks, offering real (less risky) alternatives, and managing those risks so that they do not negatively impact the consumer."

An article by the ACA[137] states that a central concern with electronic non-cash transactions, from a commercial or business perspective, is the notion of non-repudiation and being able to enforce a transaction (ie that consumers cannot repudiate a transaction once they have committed to it). In cash transactions this is not an issue because the business has already obtained the money for the goods or service:

> ...in the traditional domain there exists a continuum of identification that relates to the commercial 'strength' of the transaction. Discussions of electronic identification sometimes ignore this idea of varying strength identification. This leads to a polarised view of identity, with many technologists favouring a single robust identity for an individual.

The ACA add:

> A continuum of identity can be sketched to chart the types of identity that may be useful in different circumstances. This ranges from identification highly authenticated by third parties to unidentifiable aggregated statistical information. As a way of describing the strength of identification at the highly authenticated end of the spectrum, the points-based checking system used to summarise evidence of identity checks has been adopted as a short hand. So a 100-point check has become a standard way of describing a strong identity, sufficient for instance to open a bank account.
>
> However it is worth noting even in this area there is a range – for instance it is quite possible to develop and use a 50-point check for some circumstances, while for others a higher bar can be imposed using a 300-point requirement. Beyond this, one moves into the realm of positive vetting employed by national security agencies...[138]

---

137 ACA, *The proof of who I am*, October 2001. Available at http://www.choice.com.au under articles. (accessed March 2003)

138 ACA, *The proof of who I am: Are we being 'over identified' as we move around the marketplace?*, October 2001. Available at http://www.choice.com.au under articles. (accessed March 2003)

The ACA also raise serious concerns about biometric technology, as well as common fears surrounding the technology:

> What is alarming is that the same technology...[biometric authentication]...is also a candidate for implantation, forming a direct connection between the physiological identity of the person and the electronic world that wants to know who they are. Those developing implants for humans to monitor a wearer's location, pulse, blood-oxygen level and other vital bodily functions have also described them as an identifier for e-commerce, capable of sending a signal from the person wearing the device to either their computer or the e-merchant with whom they are doing business, thus verifying their identity. Not only could such a device identify you, it could reveal your emotional reactions and state of mind. Not an encouraging environment for negotiation.
>
> It is exactly this fear of bodily invasion that informs a lot of the fear that is associated with biometric methods of identification. Fingerprinting is one of the most common and visible methods of biometric identification. Unfortunately for those eager to press such forms of measurement into general commercial use, it is also heavily tainted with the idea of criminality. Most ordinary consumers would vigorously object to being fingerprinted to open a bank account for instance. Once a biometric identifier has been broken or impersonated successfully – and no one can guarantee absolute security for any method of identification – eradicating the identity that has been corrupted, and re-establishing a viable identity to transact with the world again, could prove traumatic. This illustrates once again, in a dramatic fashion, that increased strength of authentication does not confer an automatic increase in the degree of security.[139]

CONCLUSION

Fraud, in particular identity fraud, has become one of the fastest growing crimes in Australia. The monetary cost to industry and the community is great. Due to the nature of this crime the responsibility for prevention and detection lies not solely with any particular agency or group but with a complex mix of public sector state and federal law enforcement agencies as well as private sector organisations. Private sector organisations play a significant role in taking steps to minimise or prevent fraud through their own procedures and practices. To date it appears that the steps taken to minimise and prevent fraud have not been entirely successful. This is probably due in part: to the self-regulatory nature of fraud prevention practices in the private sector and the reluctance of industry (as demonstrated in the KPMG survey) to implement basic fraud prevention measures in the

---

139 ACA, *The proof of who I am: Biometric authentication* October 2001. Available at http://www.choice.com.au under articles. (accessed March 2003)

first instance; and to rapidly evolving technology which creates further challenges for fraud prevention and detection.

APPENDIX A – CRIME STATISTICS

Recorded criminal incidents for fraud, 1999-2002, according to statistical division[140]

	1999		2000		2001		2002	
Statistical Division where offence occurred	***Number***	***Rate per 100,000 pop'n***	***Number***	***Rate per 100,000 pop'n***	***Number***	***Rate per 100,000 pop'n***	***Number***	***Rate per 100,000 pop'n***
Sydney	18,211	451.7	18,842	461.3	24,920	601.8	25,575	617.6
Hunter	1,728	302.4	2,110	365.8	1,926	330.9	2,226	382.5
Illawarra	907	235.8	1,145	294.2	1,303	331.3	1,261	320.6
Richmond-Tweed	890	426.3	711	336.7	749	352.0	842	395.7
Mid-North Coast	1,205	445.1	1,244	455.8	925	336.3	979	355.9
Northern	725	415.4	580	334.9	427	247.9	503	292.0
North Western	775	661.0	369	315.7	395	339.2	402	345.2
Central West	614	355.0	668	386.7	614	354.4	530	305.9
South Eastern	592	326.7	700	383.7	720	390.4	613	332.4
Murrumbidgee	777	522.8	721	484.8	940	631.7	578	388.4
Murray	485	439.0	457	415.7	351	318.7	368	334.2
Far West	80	330.7	53	224.7	50	215.5	64	275.9
NSW	**27,011**	**422.3**	**27,607**	**427.2**	**33,328**	**510.2**	**33,947**	**519.7**

[140] BOCSAR, *New South Wales Recorded Crime Statistics 2001,* 2002, Table 4.16 at p 56; BOCSAR, *New South Wales Recorded Crime Statistics 2002*, 2003, Table 4.16 at p 59. Note: there are some differences in the data for 2001 in that higher figures are shown in the Crime Statistics 2002 than in the Crime Statistics for 2001. The later figures are included here. In the explanatory notes it explains that because the reporting date and recording date of an incident may differ there is a possibility that some updating of data can occur. BOCSAR notes that "data extracted for a specified period of time (incidents reported in 2000, for example), may differ according to the date of extraction of the data".

Number of charges for deception and related offences – NSW Local Court – 1997 to 2001[141]

	1997	1998	1999	2000	2001
Fraud, forgery or false financial instruments	5011	5321	6561	6502	8778
Counterfeiting currency and related offences	26	15	41	17	39
Dishonest conversion	1234	1208	1243	1234	1532
Bribery	33	42	33	28	32
Other deception offences	99	91	114	102	174

Number of charges for deception and related offences - NSW Higher Courts - 1997 to 2001[142]

	1997	1998	1999	2000	2001
Fraud, forgery or false financial instruments	408	395	270	354	277
Counterfeiting currency and related offences	4	9	0	5	10
Dishonest conversion	114	66	52	61	61
Bribery	13	11	12	19	0
Other deception offences	21	7	9	12	9

141 BOCSAR, *Number of charges by offence type, NSW Local Court, 1997 to 2001*, at http://www.agd.nsw.gov.au/bocsar1.nsf/pages/lc_charges9701, accessed 3 February 2003.

142 BOCSAR, *Number of charges by offence type, NSW Higher Courts, 1997 to 2001*, at http://www.agd.nsw.gov.au/bocsar1.nsf/pages/hc_charges9701, accessed 3 February 2003.

Penalties for principal offence -deception and related offences– Local Court Statistics 2001

	Fraud forgery or false financial instruments	Counterfeiting currency or related offences	Dishonest conversion	Bribery	Other deception offences	TL
imprisonment	198	4	23	1	1	**227**
home detention	14	-	2	-	-	**16**
periodic detention	79	-	12	-	-	**91**
suspended sentence	121	-	21	-	1	**143**
community service order	427	1	71	1	1	**501**
bond with supervision	160	-	63	-	2	**225**
bond without supervision	413	2	110	2	4	**531**
bond without conviction	136	-	100	1	4	**241**
fine	531	6	160	3	32	**732**
licence disqualification	-	-	-	-	-	**-**
compensation	26	-	9	-	-	**35**
nominal sentence	18	-	2	-	1	**21**
no conviction recorded	80	-	37	1	3	**121**
total	**2,203**	**13**	**610**	**9**	**49**	**2,884**

Penalties for principal offence -deception and related offences– Higher Court Statistics 2001

	Fraud forgery or false financial instruments	Counterfeiting currency or related offences	Dishonest conversion	Other deception offences	TL
imprisonment	60	1	17	4	**82**
home detention	1	-	1	-	**2**
detention in juvenile institution	-	-	-	-	**-**
periodic detention	7	1	6	-	**14**
suspended sentence with supervision	5	-	-	-	**5**
suspended sentence	7	-	4	-	**11**
community service order	5	-	1	-	**6**
bond with supervision	5	-	3	-	**8**
bond without supervision	7	1	-	1	**9**
bond without conviction	1	-	-	-	**1**
fine	1	-	-	-	**1**
rising of the court	1	-	-	-	**1**
no conviction recorded		-	1	-	**1**
total	**100**	**3**	**33**	**5**	**141**