Cards Australasia 2003
Melbourne Convention Centre
3 September 2003

"Addressing Identity-related Fraud"

Russell G. Smith
Australian Institute of Criminology

INTRODUCTION

In the twenty-first century, criminal misuse of identity lies at the heart of most plastic card fraud, whether it involves opening credit card accounts in false names, providing misleading information as to credit-worthiness, or using stolen cards without authorisation. Card-not-present transactions such as those that take place by telephone or on-line also create opportunities for identity fraud unless adequate verification of the identity of the card holder can take place. Finally, counterfeiting and altering plastic cards is one of the mainstays of identity fraudsters.

This paper examines the problem of identity fraud as it relates to card-based payment systems. After considering some of the drivers behind the increase in identity-related fraud, some evidence is provided of the extent of the problem and its effects on business and government. The paper concludes with an examination of three key issues in controlling identity-related fraud—reforming the points-based system of identification; establishing a national identification system; and using biometric authentication and verification systems as a substitute for knowledge-based approaches.

UNDERSTANDING THE RISKS OF IDENTITY FRAUD

The methods used to perpetrate identity-related fraud are many and varied, although they can be grouped into two main categories: creating an entirely fictitious identity, or making use of someone else's identity without their knowledge or permission. The motivation in each case is to obtain a financial gain or other benefit or to avoid a liability and then be unable to be located by police or regulators. This usually also involves opening and using bank accounts in false names so that stolen funds can be deposited anonymously.

Identity Theft Case Study

In March this year, a case was reported in the media in England that provides a good example of the problem of trans-national identity-related fraud. The case concerned a 72 year-old man, Derek Lloyd Sykes, whom the FBI were

investigating in connection with alleged telemarketing fraud involving millions of dollars in the United States.

Since 1989, Sykes had been making use of the identity of a 72-year old retired businessman from Bristol in the UK, Derek Bond, who had never met Derek Sykes, and had no connection with his alleged crimes at all. The FBI issued a warrant for the arrest of Derek Sykes and this was executed by South African Police in Durban on 6 February 2003 in the name of Derek Bond. Unfortunately, Derek Bond, the retired businessman, who was on holiday with his wife, was arrested instead of Derek Sykes.

The police relied on the fact that the warrant was in the name of Mr Bond, he was the correct age, looked similar, and had the same passport number. Mr Bond was held in custody at police headquarters in Durban until 26 February 2003 when he was released following the arrest of the real suspect, Derek Sykes, the day before in Las Vegas. Mr Bond is now planning to sue the FBI for wrongful arrest and detention for three weeks in South Africa (BBC News 2003). The case highlights the kinds of problems that arise when a person's identity is made use of by someone else for illegal purposes.

The Importance of Identification

The commission of financial crime through the creation and use of misleading and deceptive identities is one of the most pressing concerns that government agencies and the private sector have faced in recent years.

Identifying people with certainty is both a time-consuming and costly activity for public sector agencies as governments need to know with certainty to whom benefits should be paid and from whom revenue should be collected. For example, the Australian Taxation Office issues about 500,000 tax file numbers each year, Centrelink processes over 4 million new claims or re-grants of benefits, there are approximately 500,000 new Australian residents that need to be processed each year through births, permanent new arrivals and long-term visitors, the Department of Foreign Affairs and Trade issued nearly 1 million passports in 2001-2, and in the year 2001, the Australian Electoral Commission also processed 2.6 million enrolment forms and amendments, and more than 12.6 million Australians were registered to vote in the last federal election. On each occasion, proof of identity procedures had to be complied with.

In the private sector, the task of establishing identity is similarly extensive. In the year 2002, for example, there were 785 million ATM transactions and 766 million EFTPOS transactions in Australia, each of which required customers to identify themselves by entering a PIN. Logging onto computers, registering businesses

and companies, and entering into contracts (such as contracts for telecommunications services) also requires proof of identity, although sometimes less demanding requirements for proof of identity are required. Each of these occasions provides an opportunity for fraudsters to begin the process of misappropriating someone's identity.

Identity Fraud Involving Plastic Cards

In the realm of plastic cards, identity fraud raises considerable problems as plastic cards continue to become more prevalent and used to verify the legitimacy of the holder in a wide range of applications. Some examples of identity fraud risks in connection with card usage are as follows.

On 3 October 2003, a 32-year-old man, Abraham Abdallah, in the United States, pleaded guilty to a 12-count indictment alleging wire fraud, mail and credit card fraud, identity theft and conspiracy. These charges related to attempts to transfer more than US$80 million from the accounts of his victims by requesting electronic funds transfers and securities transfers into fraudulently opened accounts, and by depositing counterfeit cheques into these accounts.

The accounts were opened from his local library's computer in Brooklyn in the names of various famous media personalities. To open these accounts he gave personal information that he had obtained by sending forged letters of major broking houses to credit agencies requesting the financial history of each of his victims. Fortunately, a bank contacted one of the victims asking him to confirm a suspicious request to move US$10m from one of his accounts.

When he was arrested in March 2002, police found photographs, Social Security numbers, dates of birth and addresses of more than 200 CEOs of large organisations, and more than 400 credit card numbers with matching addresses and personal information on his computer. He was also found to have 800 fraudulent credit cards and 20,000 blank credit cards in his possession (Burkeman 2002).

In Australia, a more successful offender used desk-top publishing equipment to create forty-one birth certificates, forty-one student identification cards, some containing photographs, each in separate names, and a counterfeit driver's licence in Victoria between August 1995 and March 1996. These were used to open forty-two separate bank accounts throughout the Melbourne metropolitan region, to pay cheques into accounts as wages and make immediate withdrawals before they had cleared, to register a business name, to obtain sales tax refunds, and to defraud various retailers. The offender was convicted of a variety of offences and sentenced to five years' imprisonment with a non-parole period of three years. He

was also ordered to pay compensation of $41,300 and reparation to the Commonwealth of Australia in the sum of $458,383 (R v *Zehir* Court of Appeal, Supreme Court of Victoria, 1 December 1998).

Fraud risks have also arisen in connection with Centrelink's Electronic Benefits Transfer (EBT) system that was introduced in 1997 and which now operates nationally to deliver limited social security benefits replacing the traditional counter cheque. Operated with a PIN, the genuine Centrelink client is issued with a one-time use debit card and a PIN to draw cash from ATMs. Once the card's value is exhausted the client should destroy the card. Since the system was established a number of former Centrelink employees have been convicted of fraudulently using the EBT computer system to defraud the Commonwealth (Warton 1999). In one case a former employee of Centrelink used his computer logon identification fraudulently so as to cause EBT cards to be issued by the computer system in the names of certain pensioners, who were unaware that this had been done. The EBT cards purported to entitle the identified pensioners to credits of various amounts. The offender then used ATMs to withdraw cash amounting to $20,190. He was found guilty in respect of a number of counts and sentenced to imprisonment in the aggregate for three years and nine months with a non-parole period of two years six months and with a reparation order of $20,190 in favour of the Commonwealth (R. v *Thompson* [2002] NSWCCA 149 (16 May 2002, New South Wales Court of Criminal Appeal).

ASSESSING THE LEVELS AND GROWTH OF IDENTITY FRAUD IN AUSTRALIA

Determining the size of the problem of identity-related fraud can be approached from a number of perspectives, each of which has its own problems and limitations.

Official Statistics

Official statistics concerning the number of crimes recorded by police provide one indication, although there is no single category of identity-related fraud and so it becomes very difficult to count the number of relevant crimes involved. Even determining the exact number of fraud offences in each State, Territory and the Commonwealth is extremely difficult as there are many hundreds of offences that have an element of fraud or dishonesty to them, and these differ across jurisdictions.

Victimisation Surveys

The alternative approach is to conduct surveys of organisations and individuals that have experienced identity-related fraud and ask them to report the nature and extent of their victimisation. Unfortunately, surveys of individual consumers and businesses tend not to ask about the means by which fraud offences were perpetrated and so existing surveys provide limited information on the extent of the problem of identity-related fraud.

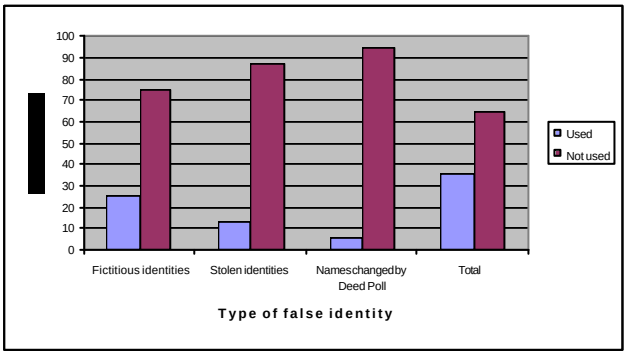
In the European Union, plastic card counterfeiting is estimated to cost EUR600 million or 0.07 per cent of industry turnover (Lakeman 2001), although much of the increase in plastic card fraud has related to card not present transactions conducted by telephone and the Internet. In the United Kingdom, card fraud cost £189 million in 1999 or 0.117 per cent of industry turnover (Levi 2000).

In Australia, there have been a number of recent attempts to study fraud and identity fraud in greater detail.

AIC / PricewaterhouseCoopers Serious Fraud Study

In a study undertaken by the Australian Institute of Criminology and PricewaterhouseCoopers (2003) of 155 serious fraud cases prosecuted in Australia and New Zealand in 1998 and 1999, it was found that fictitious identities were used in approximately one quarter of the files examined (24%) and stolen identities were present in 13 per cent of files. Deed Poll name changes were present in some 5% of files examined. Of the 155 files examined, 59 (38%) involved the misuse of identity in some way.

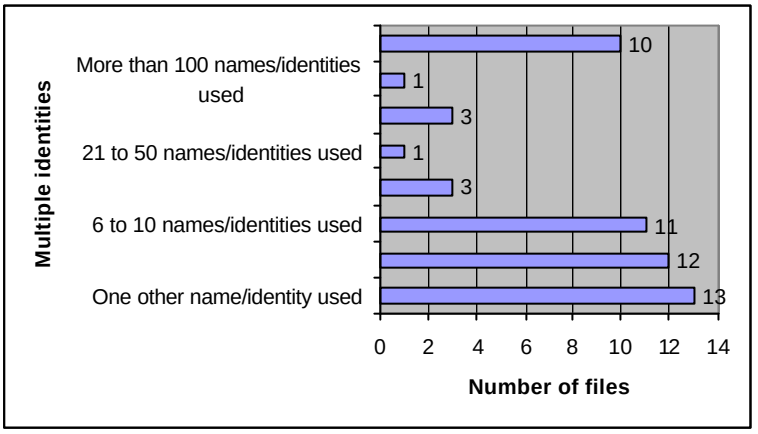
Figure 1 - Use of False Identities in Serious Fraud Cases
Australian Institute of Criminology and PricewaterhouseCoopers (2003)



Although these data show a much lower incidence of false identities than has been discussed in very recent times in the media, the present data reflect conduct that took place some years ago (even back to the early 1980s) when misuse of identity was less prevalent due to the limited availability of computers, which are now of central importance in the fabrication of false proof of identity documents.

Arguably of greater concern, however, was the use of multiple false identities by offenders. In 47 files information was recorded on the number of false names or identities used by offenders.

Figure 2
Number of Multiple Identities Used by Offenders
Australian Institute of Criminology and PricewaterhouseCoopers (2003)



The majority of files in which false names or identities were used entailed the use of one or two false names or identities, although one file involved an offender using 116 different names or identities. It can be expected that as the use of desk-top publishing equipment increases, the use of large numbers of false identities will also increase as it is just as simple to fabricate one as many false documents to misrepresent one's identity.

Birth Registry Studies

Studies have been conducted in both New South Wales and Victoria in which birth certificates used to open bank accounts have been verified with the relevant Registries.

The NSW Registrar of Births, Deaths and Marriages carried out a trial verifying birth certificates tendered to Westpac to open bank accounts. It was found that 13% of birth certificates presented were not an exact match with the records held

by the issuing authority. In Victoria, in a similar study, 18% of birth certificates tendered did not correspond with information held by the Office of Births, Deaths and Marriages.

WHAT IS THE OVERALL IMPACT ON BUSINESS AND GOVERNMENT?

The impact that identity-related fraud can have on business and government is extensive. On occasions businesses may be forced to close or governments may lose a considerable proportion of their revenue. The consequences of identity-related fraud fall into the following categories.

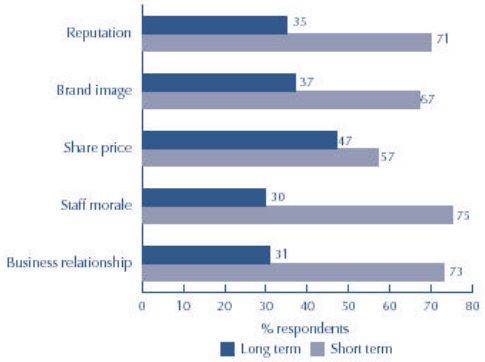
Direct Financial Loss

The most obvious consequence is money actually stolen or revenue lost through fraud. The Australian Institute of Criminology has recently estimated the national cost of fraud in Australia to be $5.88 billion a year (Mayhew 2003). Even if we use the estimate from the AIC/PwC study that identity-related fraud accounted for 38% of all serious fraud cases, this would mean that identity fraud would be costing $2.2 billion a year in Australia.

Indirect Costs

There are various financial consequences that arise following the detection of fraud that may initially be hidden. The latest survey of Global Economic Crime by PricewaterhouseCoopers (2003) identified five collateral costs of fraud as being reputational damage, damage to brand and image, effects on share price, staff morale and business relationships. Figure 3 shows the percentage of the 3,623 respondents from 50 countries who considered that each of these costs had a short-term or long-term impact on their organisation.

Figure 3
Lasting Impact of Economic Crime
PricewaterhouseCoopers (2003)



In the short term, loss of staff morale was the most prevalent cost, while adverse effects on share price were considered to be the greatest long-term cost.

In addition, there are various other costs that are associated with financial crime.

Reinstatement Costs

Where computer systems have been compromised, down-time while repairs are being effected or where systems have to be un-graded or replaced, may be considerable. Replacing damaged hardware or data can involve considerable expense. Similarly, replacement of staff involves costs of advertising, interviewing and checking credentials as well as re-training.

Regulatory Non-performance

Identity deception can also lead to reduced levels of performance by regulatory agencies. Immigration controls may be circumvented, licensing requirements for firearms controls, professional registration, or motor vehicle compliance standards may all be overcome where individuals misuse proof of identity documents. This results in agencies failing to achieve their compliance targets.

Reputational Damage

An indirect consequence of fraud victimisation that is difficult to quantify in monetary terms is the damage suffered to an organisation's reputation. In the public sector this can have repercussions in terms of loss of voter support or through reluctance of the public to make use of new systems that have been shown to be vulnerable to manipulation.

One example of this involved the attack on the Australian Taxation Office's Website, GST Assist that was established following the introduction of Australia's new taxation system. A student known variously as K2 and Kelly exposed a glaring security breach in the Website. Simply by typing in a string of numbers, K2 was able to gain access to the records of more than 20,000 GST-registered providers, which contained their bank account details. He alerted more than 17,000 of the providers by sending their confidential details to them by E-mail (Dancer 2000, p. 76). Even though the problem was able to be solved, it presumably reduced public confidence in the system.

Where an organisation has suffered damage to its reputation through identity-related fraud, it may be necessary to spend money not only in solving the security problem that led to the attack but also in publicising this fact in order to repair the damage to its reputation and to restore public confidence in the system used. In

the case of individual victimisation, considerable time and money may need to be devoted to repairing one's credit rating that has been damaged through identity theft.

Investigation and Prosecution Costs

Following an incident of victimisation, organisations may need to devote considerable resources to investigating the incident and preparing evidence for use in prosecutions. This may require the use of external forensic accountants, particularly where computer systems have been involved. Staff costs arising out of preparing statements and giving evidence in court can also be considerable.

Even if a conviction is able to be obtained, the organisation may still be required to take civil recovery proceedings which might entail further investigations and costs. If proceedings are taken across jurisdictional borders, these costs can be considerable. In many cases offenders may have disposed of their assets and be unable to satisfy judgments obtained against them. For example, in the case of R v *Muir* (ACT Supreme Court, 25 September 2001), in which $8.7 million had been stolen from the Department of Finance and Administration, it was reported that some $5.5 million had not been recovered from the offender (Campbell 1999).

Fraud Prevention Costs

In order to prevent identity-related fraud organisations are required to allocate considerable sums to preventive measures. This can extend from the preparation of fraud control policies and fraud prevention advice to staff through personnel screening measures, to the development and use of a range of technological fraud prevention measures such as enhanced user authentication systems for computers. Proposals to introduce computer chip cards or biometric screening systems clearly involve substantial initial outlays.

Fraud Minimisation and Detection Costs

Organisations also have on-going costs associated with fraud minimisation and detection. The use of inter-agency data matching and neural networks to monitor transaction patterns are clearly expensive and it is often only the largest agencies that are able to make use of them to minimise fraud risk.

Training of staff in the detection of identity-related fraud is also an ongoing obligation that all agencies need to address, particularly in view of the requirements of recent government fraud control policies.

Liability and Insurance Costs

The possibility also arises that organisations that have been negligent in providing information about the identity of individuals may be sued where loss has been caused through reliance being placed on the information provided. In the private sector this has already occurred where a bank negligently issued a certificate representing that an accountant had been assessed for competency and was competent to provide professional advice (*Smith* v *State Bank of New South Wales Limited* [2001] FCA 946 (20 July 2001, Federal Court of Australia). Similarly, where organisations have been negligent in maintaining secure databases of personal information, questions of civil liability might arise. In addition, claims made on insurance policies may result in premiums rising in the future.

In all, identity fraud victimisation entails a wide range of both direct and indirect costs that are rarely taken into account when quantifying the size of the problem.

REFORMING THE POINTS-BASED SYSTEM OF IDENTIFICATION

In Australia, the *Financial Transaction Reports Act 1988* (Cth) regulates the manner in which identity must be established when accounts with financial institutions are created. Similar points-based systems operate when individuals register for secure on-line transactions (such as when they register with PKI Registration Authorities) and informal systems of identification operate when people obtain other official documents such as passports and drivers' licences.

The system is created under the *Financial Transaction Reports Regulations 1990* (Cth) for identifying people when they open accounts with financial institutions. Documents submitted as proof of identity are each assigned a value depending upon their importance and level of security. Under the Regulations documents are classified as being Primary or Secondary with the following points allocated to each: Primary documents (which carry 70 points each) include a certificate of citizenship, current passport and birth certificate. Secondary documents include a driver's licence (40 points), public employee or student ID card (40 points), credit card (25 points), Medicare card (25 points), and local council rates notice (25 points).

There is a range of other documents which can be relied on to verify one's name and address, each carrying different numbers of points. At present 100 points of documentation are required in order to open an account with a financial institution, although 150 points may be required in order to establish one's identity for the most secure forms of electronic communications with the government in the future (*Project Gatekeeper*).

Special provisions under the *Financial Transaction Reports Regulations* apply in relation to children, recent arrivals in Australia, non-residents and Aboriginal and Torres Strait Islander residents living in isolated areas (Regulations 6-9).

The legislation creates various offences for infringing these regulations. It is an offence to open an account in a false name, such as by tendering a false passport or someone else's driver's licence, or to disclose only one of two names by which a person is known. This carries a maximum penalty of 2 years' imprisonment (s. 24 *Financial Transaction Reports Act* 1988 (Cth)). It is also an offence knowingly or recklessly to make a false or misleading statement in advising a financial institution of a change of name, which carries a maximum penalty of 4 years' imprisonment (s. 21A). Penalties also apply to cash dealers who fail to comply with reporting requirements under the Act (ss. 28-34).

Reliance on the 100 point system does not, however, provide a complete solution to the problem of identity-related fraud as it is possible to submit documents which have been forged or altered. Although the 100 points system itself provides a reasonable means of establishing identity, in practice it is easy to circumvent, largely through the inability of staff whose task it is to verify documents to be able to do so quickly and accurately.

The solutions to the problem lie not so much in increasing the number of points of proof of identity documents required, but in improving the security features of documents, enabling staff who inspect documents for authenticity to be able to detect counterfeits and to verify the information contained on documents with the issuing source, and for alternative means of identification to be used, such as interviews, or biometrics.

Perhaps the most important area for improvement is inter-agency cooperation concerning the verification of proof of identity documents. At present documents used to establish identity are issued by a number of State and Commonwealth agencies. Cross-validation would enable inconsistencies to be ascertained and identity-related fraud minimised. In addition, improved identification checks are needed when corporations and businesses are registered and when accounts with public sector agencies, such as the Australian Taxation Office, are established.

On 7 July 2003, the Federal Minister for Justice and Customs (2003) announced the idea of a national "Electronic Gateway" to match data between all agencies that issue documents used for establishing identity such as Birth Certificates, Drivers' Licences, Passports etc. If this is implemented some, but by no means all, of the problems of identity fraud will be resolved.

IS A NATIONAL IDENTIFICATION SYSTEM THE ANSWER?

One solution that is sometimes advanced to the problem of identification of people by government agencies is the establishment of a single identity card linked to a national database of personal information. Technology now provides the ability to establish such a system through the use of Internet-based networks. The needs of electronic commence and electronic service delivery by government agencies also suggest that a national identity database might be beneficial.

Proposals for the introduction of national identification cards are being discussed in the United Kingdom, South Africa and a number of South-East Asian countries in order to contain the risks of identity fraud.

The problems with such a solution lie in the risk that the security of a networked identity database could be compromised and that data could be used for unauthorised purposes in breach of privacy principles. There is also the reluctance of the public to find such a solution acceptable, at least in Australia where the introduction of a national identity card has been generally opposed.

There have, however, been proposals to issue people with cards that could act as a substitute for an identity card. In New South Wales, for example, a new birth card with enhanced security features has been proposed to replace paper birth certificates.

Rather than creating a single national identification system it might arguably be better to improve the security of our main documents used to establish identity, such as birth certificates, passports, and drivers' licences and to exclude from any points-based system documents that fail to have adequate security measures in place. Verification checks between issuing agencies should also be enhanced to enable anomalies to be detected.

THE ROLE OF BIOMETRICS IN COMBATING IDENTITY FRAUD

Biometric user authentication is also attracting great interest for the apparently higher level of integrity that it offers in comparison with standard knowledge-based and token-based systems. In the future, biometric user authentication technologies may be able to enhance security considerably, although privacy concerns will need to be addressed. Already there is a wide variety of such systems being used which make use of an individual's unique physical properties. Common biometric identifiers today include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odours. Fingerprint identification

systems are now being used to restrict access to keyboards and when using a computer mouse.

Although such systems achieve much higher levels of security than those which rely upon passwords, they are expensive to introduce and raise potential problems in terms of privacy and confidentiality of the personal data stored on computer networks. An initiative designed to reduce social security fraud in Toronto has been the enactment of legislation which would enable welfare benefit recipients to use fingerprint authentication when dealing with the Ontario government in Canada. Detailed privacy protections are built into the legislation which includes requirements for all biometric data to be encrypted and for the original biometric to be destroyed after the encryption process has been completed (Cavoukian 1999).

In the wake of the September 11 attack on the United States, national security has been emphasised as a major priority in many countries. Among the measures being considered in some countries is the use of compulsory identity cards, which may or may not include a biometric identifier. It was reported in early 2002, that Hong Kong would begin issuing multi-use ID 'smartcards' to citizens from July 2003, replacing all 6.8 million existing ID cards by March 2007. They will contain basic biometric information such as thumb prints and a photograph, and will be capable of multiple functions including use as drivers' licences and as library cards (Benitez 2002).

Such proposals face vocal opposition by advocates of privacy who raise the grave consequences of essential information being misused such as occurred during the Nazi regime in the Second World War. Responding to a recent British proposal for an 'Entitlement Card' released by the Home Office in July 2002 (Home Office 2002), a consultation paper by Privacy International observed that 'no common law country in the world has ever accepted the idea of a peace-time ID card' (Privacy International 2002). However, a pilot program for a biometric ID card on a much smaller scale has already been implemented in Britain, in relation to asylum seekers.

The new card is to replace the Standard Acknowledgement Letter that is currently issued to asylum seekers as the paper document was too easy to forge, and was not durable. The government hopes that the card will reduce the scope for fraud through illegal benefits claims (McAuliffe 2002).

Biometrics, like other identification systems, is not impervious to misuse. Biometric data are kept on electronic databases which may be compromised from external hackers or by insiders. The possibility of displacement of crime could also arise with criminals compelling users to undergo biometric scanning in

circumstances of duress. Already this has occurred in connection with customers using ATMs when they have been forced to disclose their PIN under threat of violence.

Biometric systems can, however, when used in conjunction with other identification systems and in accordance with privacy laws, provide one means of reducing the risk of identity fraud. They cannot, however, be said to be a complete answer to the problem by themselves.

CONCLUSIONS

There is, arguably, no single solution to the problem of identity-related fraud, but, rather, a range of measures need to be adopted that will involve both Commonwealth and State agencies as well as organisations in the private sector all working cooperatively.

Technology will provide some solutions, such as the development of biometric identification systems, but these will not solve all of the problems as technological solutions, no matter how sophisticated, are able to be circumvented by those with the necessary skills and resources.

Adopting a range of identification strategies is likely to be most effective response coupled with appropriate sharing of information across agencies. Of greatest importance is the need to have systems in place to verify the authenticity of documents tendered as proof of identity with the issuing source such as offices of Births Deaths and Marriages, and Road Traffic agencies that issue drivers' licences. The latest security features should also be used on documents used to establish identity.

At the same time, privacy considerations need to be taken into account and legislation reviewed to keep pace with technological developments.

REFERENCES

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

Benitez, M. A. 2002, 'ID Card Contract Awarded', *South China Morning Post* (Hong Kong), 27 February, p. 2.

BBC News 2003, 'Briton May Sue After FBI Bungle', *BBC News Online (UK Edition)*, 26 February 2003,

Burkeman, O. 2002, 'New York Man Admits Internet Scam to Defraud Celebrities of $80m', *The Guardian*, 5 October 2002, http://www.guardian.co.uk/internetnews/story/0,7369,805091,00.html (visited 14 November 2002).

Campbell, R. 1999, 'DOFA Review in Wake of Alleged $8m Fraud', *Canberra Times*, 17 February, pp. 1-2.

Cavoukian, A. 1999, 'Privacy and Biometrics'. Paper presented to 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September.

Dancer, H. 2000,'K2 Uncovers GST Keyhole', *The Bulletin* (Australia), 11 July, p. 76.

Home Office, Britain 2002, *Entitlement Cards Unit Website*. http://www.homeoffice.gov.uk/dob/ecu.htm (visited 2 October 2002).

Lakeman, P. 2001, 'Mechanisms for International Cooperation: Interpol's Universal Classification System for Counterfeit Payments Cards', in Broadhurst, R. G. (ed.), *Proceedings of the Asia Cyber Crime Summit*, Hong Kong, 25 -26 April, Centre for Criminology, University of Hong Kong.

Levi, M. 2000, 'The Prevention of Plastic and Cheque Fraud', A Briefing Paper Prepared for the Home Office Research, Development and Statistics Directorate, London.

Mayhew, P. 2003, 'Counting the Costs of crime in Australia', in *Trends and Issues in Crime and Criminal Justice*, No. 243, Australian Institute of Criminology, Canberra.

McAuliffe, W. 2002, 'Asylum Seekers Get First UK Biometric ID Cards', *ZDNet Australia*, 5 February. http://www.zdnet.com.au/newstech/security/story/0,2000024985,20263301,00.htm (visited 2 October 2002).

Minister for Justice and Customs (2003), *Media Release*: Identity fraud initiative to offer better protection for Australians, 6 July. http://parlinfoweb.aph.gov.au/piweb/Repository1/Media/pressrel/4YS960.pdf

PricewaterhouseCoopers 2003, *Global Economic Crime Survey 2003*, PricewaterhouseCoopers and Wilmer, Cutler and Pickering, New York.

Privacy International 2002, *Entitlement Card Proposal FAQ.* http://www.privacyinternational.org/issues/idcard/uk/uk-idcard-faq.html (visited 2 October 2002).

R v Thompson [2002] NSWCCA 149, New South Wales Court of Criminal Appeal, 16 May 2002

R v Muir ACT Supreme Court, 25 September 2001

R v Zehir Court of Appeal, Supreme Court of Victoria, 1 December 1998

Smith v State Bank of New South Wales Limited [2001] FCA 946, Federal Court of Australia, 20 July 2001

Warton, A. 1999, 'Electronic Benefit Transfer Fraud: The Challenge for Federal Law Enforcement', *Platypus Magazine: The Journal of the Australian Federal Police*, vol. 65, December, pp. 38-44.