IIR Conferences Retail Financial Services Forum
Sydney 9 October 2003
12.00-12.30pm
'Addressing Identity-related Fraud
in the Retail Financial Services Sector'
Russell G. Smith
Australian Institute of Criminology

Introduction

In the twenty-first century, criminal misuse of identity lies at the heart of most fraud affecting financial services organisations, whether it involves opening credit card accounts in false names, providing misleading information as to credit-worthiness, transferring funds 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 the retail financial services sector. After considering some of the key risk areas, evidence is provided of the extent of the problem and how the criminal justice system is dealing with it. The paper concludes with an examination of how the points-based system of identification can be improved and what weaknesses certain technological solutions have for controlling identity-related fraud.

Identifying Key Risk Areas in the Delivery of Financial Services

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 creditors. This usually also involves opening and using bank accounts in false names so that stolen funds can be deposited and withdrawn anonymously.

Opening Accounts in False Names

The first contact that financial institutions will usually have with an identity fraudster will be when false evidence of identity is tendered when an account is opened. Often this will be a driver's licence or birth certificate. In recent trials conducted in New South Wales and Victoria it was found that 13% and 18%, respectively of birth certificates used to open accounts with a bank did not correspond with the data held by the Offices of Births Deaths and Marriages in each state.

Often a number of identities are created so that multiple accounts can be opened. In one case in Victoria in 1996, for example, an individual created false documents that he used to establish 43 separate identities. He produced 41 false birth certificates, 41 false student identification cards, some containing photographs, and a photo driver's licence. These were used to open 42 separate bank accounts throughout Melbourne, pay cheques into accounts as wages and make immediate withdrawals, register a business name, obtain Sales Tax refunds amounting to $458,383, as well as defrauding various retailers.

He was 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 $458,383 (R v *Zehir*, Victorian Court of Appeal, 1 December 1998).

Obtaining Credit Using False Information

Often the object of opening an account in a false name is to obtain access to a line of credit, to withdraw funds, and be unable to be located for recovery purposes. In a South Australian case in 1999, an offender opened accounts with 12 financial institutions using names other than his own. He was charged with offences under the *Financial Transaction Reports Act* 1998 (Cth) of opening and operating an account under a false name. He had produced documents containing false identification such as Medicare cards, birth certificates and references from purported employers. He would then make a deposit in the account and apply for a loan to upgrade his furniture, repair a boat or purchase goods. The deposit of his own money was then withdrawn and paid into accounts opened by an accomplice under another name. He fraudulently obtained approximately $79,000. He was sentenced to 4 years' imprisonment with a non parole period of 2 years, although the non-parole period was reduced to 18 months on appeal (*Dermish* v *Commonwealth DPP* [1999] SASC 98, South Australian Court of Appeal, 18 March 1999).

In another case, an offender engaged in a systematic scheme of defrauding banks, by using false documents to establish various identities in order to sell and purchase real estate, open bank accounts and obtain loans. His activities took place from late 1996 until his arrest in May 1998. He was convicted on 21 charges of using an instrument which he knew to be false with the intention of inducing another person to accept the instrument as genuine. Nineteen of the instruments were bank loan applications or other bank documents. One was a birth certificate and one a driver's licence. The loss to the banks arising out of these transactions was around $4 million, and the gain to the appellant almost $1.5 million, although it seems that in large part this was dissipated either in gambling or by remission to his former wife in Greece. Approximately $750,000 was able to be seized from bank accounts he controlled at about the time of his arrest. His appeal against a 6-year sentence was unsuccessful (R v *Vasil* [2000] NSWCCA 421, NSW Court of Criminal Appeal, 11 October 2000).

Cheque-related Identity Fraud

Sometimes fraudulently opened accounts will be used to launder stolen cheques. One recent case involved a Malaysian national who came to Australia on a tourist visa.

During December 1999 he was party to a scheme of banking stolen cheques by using false identities and then withdrawing the funds. The scheme was relatively sophisticated, using a number of accounts at different banks. Some of the stolen cheques used had a face value of over one million dollars. He was convicted on six counts relating to the obtaining of about $138,000 and two offences involving fraudulent cheques. His appeal against a sentence of 4 years' imprisonment with a non-parole period of 3 years was unsuccessful (R v *Keong* [2001] NSWCCA 416, NSW Court of Criminal Appeal, 12 October 2001).

Exceeding Credit Limits

Often accounts will be opened in false names in order to obtain a credit facility which is then abused. One Victorian case concerned fraud involving a credit card account that took place between February and November 1997. The defendant, who was around 24 years of age at the time of committing the relevant offences, had a history of dishonesty offences dating back to an early age. By the time she came to be sentenced in the County Court for these credit card fraud offences, she had already been shown leniency on five occasions, having been given bonds, community-based orders and, most recently, a wholly suspended sentence of eight months' imprisonment for burglary and theft convictions in 1997.

The offender fraudulently obtained nine birth certificates, two drivers' licences, three Medicare cards, one Christmas Club account book and eight bank passbooks and used them to obtain credit cards. There were 61 applications made of which 45 were granted. These were made by the offender by assuming the identity of a large number of persons, some of them fictitious but many of them real, and some of them known to her from her school days.

The accounts were manipulated so as to obtain credit much in excess of the declared limit. These frauds, which involved about twelve transactions a week over a period of nine months, benefited the offender to the value of about $10,000 a month. While this was going on she was living in subsidised public housing, receiving between $250 and $300 a week from the Commonwealth by way of pension, child endowment and 'Austudy' and earning about $400 a week as a prostitute.

She continued her systematic frauds in September, October and November 1997, notwithstanding that on 13 September 1997 the police had arrested her, searched her premises, seized numerous documents and interviewed her in relation to some of her credit card frauds. In that interview she falsely denied her own guilt and attributed the use of the card to an innocent woman whose identity she had assumed at one stage.

The committal for trial had been on 102 charges, compressed into a presentment containing 12 counts of obtaining property by deception. On 19 November 1998 there was a plea of guilty to the first nine counts, the last three having been deleted by arrangement. Each offence carried a maximum penalty of 10 years' imprisonment. On the following day she was convicted and sentenced to 12 months' imprisonment on each

count and cumulation orders were made of three months in respect of counts 2 to 9 so as to give a total effective sentence of three years, with a non-parole period of two.

The three-year sentence became the subject of an application for leave to appeal. Mr Justice Brooking observed that the offender systematically engaged in credit card fraud to obtain large amounts of cash and many and varied goods and services, and her claim to a psychologist that she personally obtained little benefit and was concerned only to keep her household running and to clothe her infant son was unreliable. The sophistication of the offences, the 'catastrophic effects of the frauds on some of those whose names were used' and the 'entire absence of remorse' exhibited by the offender were remarked on. At a more general level, the judge observed: 'the credit card has achieved ever-increasing popularity. For good or ill, it has for many people largely replaced cash as a means of payment. It has itself become an important source of cash advances. This case shows how someone can systematically abuse the system by fraudulently obtaining a stock of these plastic cards which stand in the place of money, and shows some of the injurious consequences of that abuse. Generally speaking, the kind of conduct disclosed here must attract severe punishment.' The sentence was not found to be manifestly excessive and the application for leave to appeal failed (*R v H* [1999] VSCA 182 (Supreme Court of Victoria, Court of Appeal, unreported judgment, No. 296 of 1998, 9 November 1999).

Obtaining Business Finance

One case in Queensland related to dishonest dealings with various documents in the course of business, taking place between October 1994 and June 1997. The offender was born in Hong Kong on 24 June 1943. He came to Australia with his wife and children in 1977 and, apart from a period of imprisonment, was involved in restaurant and catering businesses. In about 1994 the offender, his wife, and a couple named Chan apparently commenced a restaurant business, which owned a number of restaurants, through a company called Kung Food Catering Pty Ltd. At the relevant time he was an undischarged bankrupt and had a number of convictions, and he was therefore not entitled to become a director of a company.

Various documents were fabricated by the offender to conceal his ineligibility to act as director, and several bank guarantees were signed by the offender in the names of the other directors, the Chans, to enable the business to obtain bank loans. When it subsequently went into liquidation, the bank was unable to enforce the guarantees against the Chans and was left with a debt of $52,000 from total advances of $100,000. At the time of committing these frauds the offender was on parole for offences of armed robbery in company and kidnapping for ransom, for which he had been sentenced to 10 years' imprisonment in February 1990.

The offender assumed a false name, as did his wife, and false drivers' licences and passports were used to that end. In those false names he and his wife became directors of the company. Mr and Mrs Chan were also made directors of the company. The offender signed four guarantee documents in the names of Mr and Mrs Chan, in 1994, 1995 and

twice in 1996, for the purpose of obtaining bank loans. He also signed company minutes, purporting to authorise the borrowings, in the names of the Chans.

The offender pleaded guilty in respect of a total of 10 offences, seven of signing a document in the name of another without authority with intent to defraud, two of uttering a false document and one of forgery. He was sentenced to 18 months' imprisonment, wholly suspended for an operational period of four years, in respect of was the first count of making a document without authority, and 240 hours' community service in respect of each of the other counts.

The Attorney-General appealed against those sentences, but the court was not asked to make any custodial sentence imposed cumulative on the one being served already by the offender. Mr Justice Davies agreed with the sentencing judge that the facts showed the offending was not the most serious variety; not being 'a calculated exercise in defrauding the bank'. Several agreed facts were found to count in the offender's favour, including that if asked, the Chans would have signed the documents. However, it was found that the judge was too lenient in imposing a suspended sentence, as he was apparently reluctant to send the offender back to serve the remaining five-and-a-half years of his earlier sentence. Mr Justice Davies remarked that a non-custodial sentence in this case would be 'manifestly adequate', and substituted a sentence of 18 months' imprisonment on four of the counts, and six months on each of the others, all to be served concurrently with the balance of the sentence already being served by the offender. No recommendation as to parole was made by the Court of Appeal (*R v H*; *ex parte Attorney-General* [2000] QCA 283 (Supreme Court of Queensland, Court of Appeal, No. 114 of 2000, 21 July 2000).

Funds Transfer Fraud

Facsimile machines and personal computers are also being used dishonestly by clients to transmit fraudulent instructions to financial institutions. High quality, and relatively cheap desktop publishing facilities are widely available through the use of personal computers, scanners, and laser printers which enable near perfect copies of legitimate business documents to be produced. Many of these contain signatures of company officials which have been scanned from annual reports or other official papers. The resulting document, once transmitted to a financial institution electronically, may result in funds being remitted, usually offshore, via some irrevocable channel such as the SWIFT system of electronic funds transfer, making recovery difficult. In recent years, a number of cases involving organised groups using this simple technique have resulted in substantial losses being incurred by financial institutions.

The imperative to compete in a rapidly-changing market has placed considerable strains on financial institutions to limit time-consuming validation and verification checks. Electronic commerce, for example, demands that transactions be executed instantaneously and that payment be provided immediately. This pressure has presented new opportunities for those seeking to benefit through fraud at the transactional level (Chapman and Smith 2001).

Valuation Fraud

Financial institutions can also be defrauded by applicants for housing finance supplying false information concerning the value of the property to be purchased with money being lent on the basis of inflated property prices, or false information concerning the financial standing of the loan applicant.

One large-scale example was the case of R v *Jenkins* ([2000] VSC 503 Supreme Court of Victoria, 20 November 2000), in which the offender obtained loans and a guarantee from a lending institution in Victoria for the sum of $165 million over some 15 months from 4 May 1988 to 21 August 1989. The offender was found guilty of five counts of furnishing false information and five counts of obtaining a financial advantage by deception involving false representations in valuation reports of properties he had purchased and on the security of which he sought, and obtained, the loans. In sentencing the offender to seven years' imprisonment, with a non-parole period of three and a half years, Mr Justice Coldrey referred to the fact that the offender had been assisted in plundering the funds of the lending institution by the conduct of a dishonest and voracious mortgage broker, a dishonest and compliant valuer, and persons in positions of responsibility at the lending institution whose negligence and commercial recklessness ill served the members of the organisation.

On-line Banking Fraud

Identity fraud also arises in connection with eCommerce activities of financial institutions. Attempts have been made to deceive consumers into entering into contractual arrangements with dishonest organisations that pretend to be legitimate banks, or persuading them to provide personal information electronically. This can take place through the use of misleading domain names or so-called mirror websites.

In 2000, an attempt was made to duplicate the website of leading online payment service PayPal, under the very similar URL www.paypai.com (using a capital 'I'), so as to capture unwitting users' personal information (Sorkin 2001, p. 18).

A related problem concerns mirror web sites which are created by offenders to deceive consumers into disclosing credit card details when making purchases. In New South Wales, such a case has been investigated in which the offenders copied official Web sites of premier entertainment venues to almost every detail, including theatre layouts and restaurant information. Programs were constantly up-dated to maintain the façade of legitimacy. The crucial difference was that the fictitious site had its own credit card booking arrangement, so that customers' money would be credited to the offender's account. The bogus site for Sydney appeared on the Internet with a similar URL to the genuine site. The offenders have created 23 similar sites mirroring opera houses in Europe, including Paris and Vienna. The computer crime unit of the New South Wales Police Commercial Crime Agency contacted the FBI after tracing the bogus site to a

Miami Internet server. Since then, the server re-located to California (Sydney Morning Herald 2002).

Other frauds have also involved offenders sending out e-mail messages purporting to come from legitimate banks asking their customers to visit a Website to confirm their personal information. The unsuspecting user then is directed to an illegitimate Website and provides personal information to the offender.

Quantifying the Size of the Problem

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. Victim characteristics are also not often recorded in official statistics in sufficient detail to know, for example, which cases concerned a financial institution.

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.

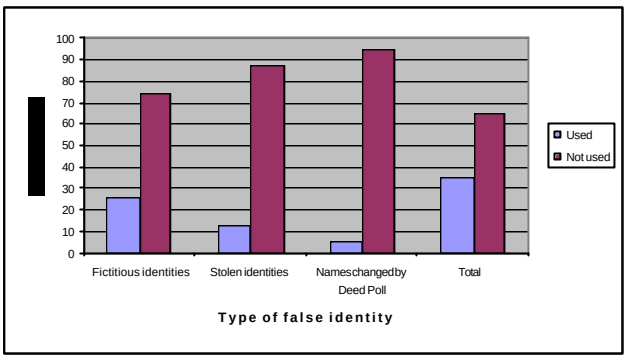
In Australia, there have been a number of recent attempts to study fraud and identity fraud in greater detail.

Australian Institute of Criminology / PricewaterhouseCoopers Serious Fraud Study

In a study undertaken by the Australian Institute of Criminology and PricewaterhouseCoopers (AIC/PwC 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

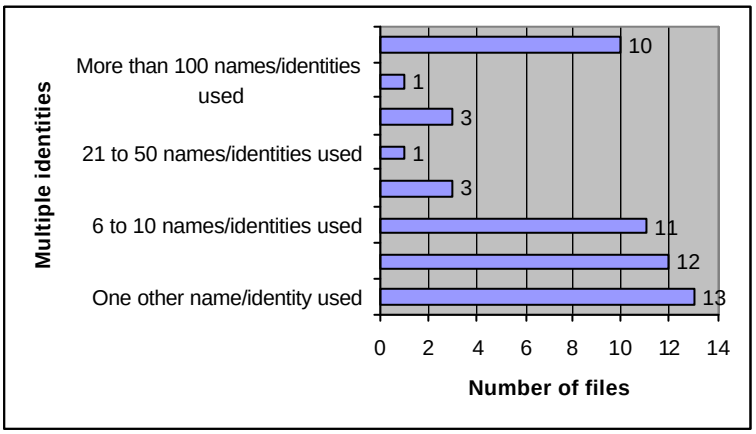
Australian Institute of Criminology and PricewaterhouseCoopers (2003)



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.

Overall, the largest number of cases of serious fraud (not just identity fraud) involved the victimisation of organisations in the financial services sector (36.2% of all victims).

Financial Cost

The AIC 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 of identity fraud being involved in 38% of serious fraud cases, this would mean that identity fraud would be costing $2.2 billion a year.

Evaluating Criminal Justice Responses

Government Responses

Government and private sector bodies throughout Australia are currently pursuing a variety of responses to the problem of identity-related fraud. Much of the interest in this issue began with a review which the House of Representatives Standing Committee on Economics, Finance and Public Administration conducted of the Australian National Audit Office's Report on the Management of Tax File Numbers, in 2000 entitled *Numbers on the Run* (House of Representatives Standing Committee on Economics, Finance and Public Administration 2000). This report found that there were 3.2 million more tax file numbers than the number of Australians at the time.

In 2001, the Commonwealth Attorney-General's Department undertook research into the problem in the form of paper *Scoping Identity Fraud* (Main and Robson 2001) while in 2002, the Australian Bureau of Criminal Intelligence (now part of the Australian Crime Commission) conducted a study of identity fraud by examining responses from 23 law enforcement and other public sector agencies, and one private sector organisation relating to identity fraud offenders, fraudulent identities and victims of identity takeovers known to them. The study identified 1,195 fraudulent identities relating to 597 suspects involving the theft of $2,639,797 (Australian Bureau of Criminal Intelligence 2002).

Also in 2002, the Australasian Centre for Policing Research produced a report *Identity Crimes Scoping Paper* (2002) and currently has a reference from the Australian Police Commissioners to examine identity crime, while the Australian Transaction Reports and Analysis Centre has a Working Party on Proof of Identity and in 2003 engaged consultants, the Securities Industry Centre for the Asia-Pacific Ltd (SIRCA), to calculate the exact cost of identity-related fraud in Australia.

The Australian Federal Police has also established an Identity Crime Task Force to assess the AFPs response to identity crimes and the National High-Tech Crime Centre is involved in coordinating law enforcement activities in relation to computer-related offences.

Legislative Issues

In Australia, a wide range of offences can be used to prosecute conduct involving misuse of identity. Each of the States and Territories and the Commonwealth has numerous offences that involve deception, dishonesty, and manipulation of documents. Some entail general crimes of dishonesty while others entail specific offences such as opening a bank account in a false name, or gaining unauthorised access to computers.

In New South Wales, the offence most directly applicable to identity-related fraud is section 184 of the *Crimes Act 1900*:

> Whosoever falsely personates, or pretends to be, some other person, with intent fraudulently to obtain any property, shall be liable to imprisonment for seven years. Nothing in this section shall prevent any person so personating, or pretending, from being proceeded against in respect of such act, or pretence, under any other enactment or at Common Law.

In the Commonwealth, the criminal law relating to economic crime was amended by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*, which commenced on 24 May 2001. Relevant offences include obtaining property or a financial advantage by deception (Division 134), fraudulent conduct (Division 135), forgery (Division 144) and falsification (Division 145). There is now a need for these model provisions to be introduced in each of the states and territories.

In addition, the Federal parliament has recently enacted the *Cybercrime Act 2001* which was assented to on 1 October 2001 and commenced on 21 December 2001. This Act inserts a new Part 10.7 – Computer Offences into the Commonwealth *Criminal Code Act 1995*. Some of the Cybercrime Act provisions could be used to prosecute identity-related frauds carried out through the misuse of computers, such as where a persons gains access to a computer by using another person's password without authorisation. Again, these model provisions need to be introduced in each of the other jurisdictions, although this is starting to occur. In Victoria, for example, the *Crimes (Property Damage and Computer Offences) Act 2003* (Vic), which was assented to on 6 May 2003 created a range of computer-based criminal offences based on the Commonwealth's *Cybercrime Act*.

In the United States, specific legislation has been introduced to deal with identity-related crime. The Federal *Identity Theft and Assumption Deterrence Act of 1998* (18 USC 1028) makes identity theft a crime with maximum penalties of up to 15 years' imprisonment and a maximum fine of US$250,000. It establishes that the person whose identity has been stolen is a victim who is able to seek restitution following a conviction. It also gives the Federal Trade Commission power to act as a clearinghouse for complaints, referrals, and resources for assistance for victims of identity theft. Some 47 American states now have some form of identity theft legislation, although the Federal Act is the most comprehensive.

In May 2002 the Federal Identity Theft Penalty Enhancement Bill 2002 was introduced, for first reading, to amend the Federal Criminal Code to establish penalties for aggravated

identity theft. This Bill was referred to the Senate Sub-Committee on Crime, Terrorism and Homeland Security on 3 June 2003.

The bill prescribes additional punishments of: two years' imprisonment for using false identities in connection with felonies relating to theft from employee benefit plans and various fraud and immigration offences, in addition to the punishment provided for such felony; and five years' imprisonment for using false identities in connection with terrorist acts, in addition to the punishment provided for such felony. The bill also bars probation for any person convicted of such violations.

In England in May 2003, it was announced that legislation would be introduced to make it a criminal offence to be in possession of false identity documents without reasonable cause. This was particularly designed to address organised criminal activities and terrorism but would also have an impact on financial crime.

The question arises as to whether Australia, or its States and Territories should enact specific identity fraud legislation. Australia already has substantial maximum penalties available for identity-related fraud offences, with terms of imprisonment of up to ten years' being provided in some jurisdictions.

Although the enactment of specific identity-related fraud legislation would provide a public statement that conduct of this nature is illegal and is being specifically addressed by governments in Australia, it would, arguably, achieve little in assisting in the prosecution of offences and in ensuring that convicted offenders receive appropriate sanctions.

Suggestions have also been made that there should be new offences created for the possession and use of equipment used to counterfeit documents with intention to act dishonestly. Examples would include embossing machines (used to emboss credit card account details onto blank credit cards), tipping machines (used to cover the embossed account details in tin foil to correspond with the laminated colour of the credit card), rolls of gold and silver tin foil, base credit cards which had not been embossed or encoded, forged credit cards embossed and/or encoded with credit card account information, encoding machines (used to encode account information onto false credit cards), Point of Sale Terminals, card skimmers (used to extract information from the electro-magnetic stripes of cards), and computers used to collect and store personal information.

It has also been suggested that the accused should bear the burden of having to prove that possession and use of such equipment was legitimate. At present possession of such equipment could form the basis of a charge of conspiracy to defraud or possession of false instruments, although this is sometimes difficult to prove intent to defraud. It remains to be seen whether legislative reforms in this area will be adopted in Australia.

Law Enforcement Issues

Even if appropriate legislation exists, there are many practical barriers to achieving a successful prosecution in cases of identity-related fraud.

The first problem is making sure that you investigate and arrest the right person. In March 2003, 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.

Gathering evidence in identity fraud cases is often difficult as it may be contained on computers, it may be encrypted, or it may be necessary to prove that the suspect was using a computer at a given time. Problems of identifying suspects are usually resolved using traditional investigative techniques, such as video surveillance or gathering indirect circumstantial evidence that locates the accused at the terminal at a particular time and day. However the use of covert surveillance is not always possible. Some investigators are beginning to use biometric means of identification. At present, few computers have biometric user authentication systems such as fingerprint scanners when logging-on.

When they become more widespread, problems of identification may be reduced, although, of course, once a person has logged-on, this does not prevent someone else from using that terminal without the person's knowledge if they are absent. DNA samples can also be gathered from keyboards which have been used to identify an individual with a particular computer in some cases. Where incriminating evidence has been encrypted, it may be necessary to use key-logging systems to find out passwords. The installation of such a program, of course, must be done without the knowledge of the accused and a special warrant needs to be obtained for this.

In one famous case in the United States, evidence obtained in this way was challenged on the grounds that the key logger involved the illegal interception of wire communications that required a special warrant. It was held, however, that the key logger only operated when the computer's modem was not connected, thus excluding any interception of

telecommunications (*United States* v *Scarfo*, 2001, Criminal No. 00-404, District of New Jersey).

Because identity fraud often does not involve face-to-face communications, it is possible for offenders and victims to be located in more than one jurisdiction. More sophisticated conspiracies may involve individuals in three or more jurisdictions within Australia or overseas. This creates problems of encouraging victims to report offences to appropriate authorities, obtaining evidence, and, where necessary, translating it into English, locating suspects and arranging for their extradition, problems of delay in using mutual assistance arrangements

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 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.

Assessing the Weaknesses of Technological Solutions

Card-based Identifiers

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 card and 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 risks that the cards could be counterfeited or altered and 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 improve the security features on documents used to establish identity such as drivers' licences and birth certificates. In New South Wales, for example, a plastic birth card with enhanced security features has been created to replace paper birth certificates. Similarly, drivers' licences now have considerably more security features built in than previously.

In addition to improving the security of documents used to establish identity, there are proposals to establish a national document verification system to ensure that counterfeit documents will be detected if they are used for dishonest purposes.

Online Payment Systems

At present, on-line payment systems have varying standards used to verify the identity of users when enrolling and when carrying out transactions. Most use a points-based system for assessing the authenticity documents used as evidence of identity, and once a user has been enrolled, transactions are generally commenced with a password.

Misuse of passwords then enables fraud to be perpetrated even if an individual has enrolled legitimately.

Even E-commerce technologies that make use of public key infrastructures and digital signatures can be manipulated simply by individuals presenting fabricated documents to support a false identity when registering with a Registration Authority in order to obtain their key pair for use in secure online transactions.

Biometrics

In order to overcome these problems of authentication through the use of passwords, biometric systems are attracting great interest for the apparently higher level of integrity that they offer 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, retinal images, and facial or hand geometry. Fingerprint identification systems are now being used to log on to computers and to gain access to mobile phones.

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).

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.

The Way Forward

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 and Territory 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

evidence 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

Australasian Centre for Policing Research 2002 *Identity Crimes Scoping Paper* Australasian Centre for Policing Research, Adelaide.

Australian Bureau of Criminal Intelligence 2002, *Identity Fraud Register Pilot: Final Report,* Australian Bureau of Criminal Intelligence, Canberra.

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.

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

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

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

Chapman, A. and Smith, R. G. 2001, 'Controlling Financial Services Fraud', *Australian Banking and Finance Law Bulletin*, vol. 17, no. 3, pp. 33-9.

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Numbers on the Run: Review of the ANAO Report No. 37 1998-99 on the Management of Tax File Numbers*, Parliament of the Commonwealth of Australia, Canberra.

Main, G. and Robson, B. 2001, *Scoping Identity Fraud: An Abridged Version of a Study of Identity Fraud Risks in Commonwealth Agencies*, Commonwealth Attorney-General's Department, Canberra

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.

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

Sydney Morning Herald 2002, 'A Scam to Bring the House Down', *Sydney Morning Herald*, 28 August. http://www.smh.com.au/cgi-bin/common/printArticle.pl?path=/articles/2002/08/27/1030053059530.html