Marcus Evans Conferences, *Corporate Fraud Strategy: Assessing the Emergence of Identity Fraud*
Sydney, 25-26 July 2002

'Examining the Legislative and Regulatory Controls on Identity Fraud in Australia'

Russell G. Smith

Understanding the Range of Activities of Identity Fraudsters that Could Lead to Prosecution

Misuse of identity lies at the heart of a wide range of criminal activities. These extend from relatively simple cases in which an individual gains access to a computer using someone else's password, to extensive deliberate fabrication of documents in order to perpetrate financial crime. Sometimes a single act of so-called identity fraud may involve the commission of numerous criminal offences under both Commonwealth and State or Territory laws. On many occasions, crimes will also be committed in numerous countries.

The following examples are illustrative of the range of activities that may be involved in the commission of identity-related fraud.

Terrorism

The alleged terrorists who destroyed the World Trade Centre were said to have used other people's names when undertaking their pilot training and when boarding the aircraft prior to 11 September 2001.

Unlawful Immigration

People who want to migrate to other countries are able to by-pass official immigration channels by engaging criminal organisations to create fictitious identities for them. In Australia, for example, one syndicate charged around A$100,000 to establish new identities for prospective immigrants. After the new identity was created, which sometimes took months or even years, the person then flew to Australia using either false documents or documents belonging to someone else, and assumed life under their new name. A different person left the country on the same documents, so that there was no record of the person who came to Australia still being here (Australian Federal Police 2001).

Those countries responsible for processing refugees from Afghanistan have been required to investigate cases in which people applying for refugee status are not, in fact, who they claim to be. Some have claimed to be legitimate refugees from

Afghanistan when in fact they came from Pakistan without any legitimate claim to refugee status (McKinnon 2002).

Fraud Involving Electronic Mail and the Internet

On-line technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity, or to make use of someone else's identity. Re-mailing services can be used to disguise one's identity when sending E-mails by stripping them of identifying information and allocating anonymous identifiers, sometime encrypted for added security. By using several re-mailing services, users can make their communications almost impossible to follow (Ellison 2001).

Anonymity can also be achieved in cyberspace using less technologically-complex means. Simply purchasing a pre-paid Internet access service from an Internet Service Provider and renting a telephone line from a carrier, each in a false name provides an easy means of achieving anonymity. Free E-mail services offered by some Internet Service Providers provide another means of securing anonymity as the user may simply register using a false name and address. In addition, the use of Internet Kiosks often permits users to send messages without disclosing their true identity. These services may be used for legal reasons associated with enhancing privacy or for illegal reasons such as evading debts or police investigation of criminal activities. At present there are few verification checks made when such services are obtained.

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 transactions. Although the subsequent transaction may be secure from hackers, the identity of the person holding the key may nonetheless be fictitious.

In a recent study of on-line anonymity, Forde and Armstrong (2002) argue that those Internet services that provide the highest levels of anonymity are most likely to be used for criminal purposes. Encrypted E-mail and Internet Relay Chat that provide higher levels of anonymity were found to be preferred by those engaging in on-line paedophile activity and hacking, while the use of the World Wide Web and File Transfer Protocols that provided weaker levels of anonymity tended to be avoided by serious criminals.

A good example of this concerns the various advance fee frauds perpetrated by a group of West Africans and others since the 1980s. Various offenders began working from Nigeria targeting victims across the globe. Confederates and other fraudsters in other African countries, the United States, Britain, Canada, Hong

Kong, and Japan then began using the same techniques. The scale of these frauds increased considerably and created a global problem for law enforcement. Between August and November 1998, Australia Post, in Sydney alone, confiscated 4.5 tonnes of advance fee correspondence which had counterfeit postage, amounting approximately to 1.8 million items. E-mail has proved to be an effective way of disseminating advance fee letters as the true identity of the sender is easy to disguise and original supporting documentation unable to be checked for authenticity (Smith, Holmes and Kaufmann 1999).

There is also no way of knowing the commercial affiliations of those on the Internet. Referees for organisations might, in fact, be individuals employed specifically to indicate their approval of the organisation in question. It is possible to choose legitimate-sounding names in order to improve one's credibility or to include domain names which are misleading. There has recently developed a practice in the United States and Canada, for example, of some organisations adopting domain names containing the names of Australian cities in order to improve their credibility—despite the fact that they have no connection at all with Australia. It is also possible to fabricate Web pages in order to attract customers to businesses that might otherwise have been overlooked or avoided (Securities and Exchange Commission 2002).

Dissemination of Obscene Materials Electronically

An illustration of the use of anonymity by a criminal organisation was uncovered during 'Operation Cathedral' by police in 1998, which led to the largest ever global seizure of paedophile material. This involved police in 15 countries who uncovered the activities of the W0nderland (sic) Club, an international network with members in Europe, North America, and Australia who used the Internet to download and exchange child pornography including real-time video images. The Club used a secure network with regularly changed passwords and encrypted content. In Europe alone, over 750,000 images were recovered from computers, along with over 750 CDs and 1,300 videos and 3,400 floppy disks. One member of the Club cooperated with police which led to approximately 100 arrests around the world in September 1998 (Australasian Centre for Policing Research 2000, p. 126).

Funds Transfer Fraud

In Australia on 25 September 2001, a financial consultant formerly contracted to the Department of Finance and Administration was convicted of defrauding the Australian government by transferring A$8.7 million electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He

was also able to obscure an audit trial through the use of other employees' logon codes and passwords. He was sentenced to 7 years and six months' imprisonment with a non-parole period of 3 years and six months (R v *Muir*, ACT Supreme Court, 25 September 2001).

Between June and October 1994, a group of Russian computer hackers attempted to steal approximately US$10.7 million from various Citibank customers' accounts in the United States by manipulating its computerised funds transfer system. One offender, Vladimir L. Levin, was working in a Russian firm, and gained access over 40 times to Citibank's funds transfer system using a personal computer and stolen passwords and account identification numbers. Using a computer terminal in his employer's office in St Petersburg, he authorised transfers of funds from Citibank's head office in New Jersey to accounts which he and his co-conspirators held in California, Finland, Germany, the Netherlands, Switzerland, and Israel. Levin was arrested at Stansted Airport, in England in 1995 and, after protracted legal proceedings which went to the House of Lords, he was extradited to stand trial before the Federal District Court in New York's Southern District. In 1998, he pleaded guilty to conspiracy to defraud and was sentenced to 36 months' imprisonment and to pay Citibank US$240,015 in restitution. Citibank was able to recover all but $240,000 of the $10.7 million worth of illegally transferred funds. None of the bank's depositors lost money. The consequences for Citibank's business reputation were considerable (R. v *Governor of Brixton Prison*; *Ex parte Levin* [1996] 3 WLR 657; *In re Levin* House of Lords, 19 June 1997).

Health Benefits Fraud

Identity-related fraud risks for the Health Insurance Commission relate to the possibility of claim forms being counterfeited or manipulated so that benefits can be claimed illegitimately or funds illegally obtained. As claims continue to be processed electronically, digital signatures could be compromised, and electronic funds transfers altered or diverted away from legitimate recipients. Fraud can be committed by members of the public, health care providers, or staff of the commission.

In 1997, for example, two former HIC employees were convicted of defrauding the Commonwealth by creating false provider accounts and making illegal claims to the combined value of more than $45,000 (Health Insurance Commission, Annual Report 1996-97, Professional Review Supplement, p. 23)

Social Security Fraud

Centrelink introduced its Electronic Benefits Transfer (EBT) system in 1997 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.

Between December 1997 and January 1998, government employees fraudulently used the EBT computer system to defraud the Commonwealth. EBT cards were issued in fictitious names enabling the offenders to draw cash from ATMs. In one case, this cash was used to buy heroin in the same street as the ATM, within 10 minutes of the withdrawal (Warton 1999, p. 4). On 27 November 2001, another Centrelink employee pleaded guilty in the ACT Magistrates/ Court to similar offences involving over $8,000 (McLellan 2001).

Corporate Deception

Recent investigations by the National Crime Authority have examined false companies, represented as labour hire or service providers, used by contractors to launder cheques paid to them by their clients for the work performed. The workers did not appear on the records as employees of the contractor. In some cases they were also in receipt of social security. No group tax was deducted in respect of the payments to the workers. The contractor claimed as a deduction the payment by way of the cheques to the false company. . . . Payroll tax was avoided.

To achieve their goals the participants created companies that engaged in no legitimate trade, they created identities using false birth certificates, and as the scheme continued to evolve those who joined were provided with a kit containing all that they would need for the false identities, and to meet the requirements of the *Financial Transaction Reports Act 1988* (Cth) when opening the bank accounts needed to negotiate the cheques from the clients.

All was achieved with remarkable ease because of the opportunity the participants had to create the false identities required to make their scheme work. In some instances false documents, once accepted by agencies and institutions, resulted in the issue of genuine documents albeit in respect of a false identity. These genuine documents could ultimately be used for the issue of further genuine documents in respect of the same false identity from other agencies and institutions thereby increasing the apparent reliability of the material presented to establish the identify to the satisfaction of requirements such as are found in the *Financial Transaction Reports Act 1988* (Cth). This scheme has appeared in comparable forms in more than one industry and across the state borders (Bennett 2002).

Financial Services Fraud

During 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 fictitious accounts which had been 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 *D v Commonwealth DPP* [1999] SASC 98 (Court of Appeal, Supreme Court of South Australia, 18 March 1999).

Bank Loan Fraud

The offender 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 activities which led to the charges consisted of a systematic scheme of defrauding banks over a period from late 1996 to May 1998 when he was arrested. They included the use of false documents to establish false identities for documentation in relation to the sale and purchase of real estate, to open bank accounts and to obtain loans. The loss to the banks arising out of these transactions was around $4 million. The gain to the offender was $1,453,254, although it would seem that in large part this was dissipated either in gambling or by remission to his former wife in Greece. Something of the order of $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 V* [2000] NSWCCA 421 (NSW Court of Criminal Appeal, 11 October 2001).

Revenue Fraud

Cases of revenue fraud can also involve the misuse of identities.

From 1990 to 1994, an accountant submitted tax returns containing either false group certificates or false statements of earnings under six names, with most of the returns also claiming false business losses. He set up separate bank accounts to process tax cheques received under these false names and defrauded the tax office of $558,668. He was sentenced to 6 years' imprisonment with a 3 years non-parole period and a pecuniary penalty order under the *Proceeds of Crime Act 1987* (Cth) in excess of $600,000 (http://www.afp.gov.au/operations/fraudjob.htm).

In another case, between August 1995 and March 1996, an offender 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, and defraud 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*, Court of Appeal, Supreme Court of Victoria, 1 Dec 1998).

Stolen Cheque Fraud

The offender was 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 various banks. Some of the cheques used were from a quantity stolen with 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 K* [2001] NSWCCA 416 (NSW Court of Criminal Appeal, 12 October 2001).

The common feature in each of these cases is that the offenders made use of other people's identities in verbal representations, created and used false proof of identity documents, or fraudulently gained access to computers though the misuse of passwords or other access control systems.

What criminal offences, then, can such individuals be charged with?

Examining State and Territory Criminal Laws that May be Used to Prosecute Identity Fraud

In Australia, a wide range of offences can be used to prosecute conduct involving misuse of identity. Each jurisdiction has its own laws and rules governing dishonesty. Examples include theft, obtaining a financial advantage by deception, making a false instrument, fraudulent misappropriation, obtaining money by false or misleading statements, obtaining credit by fraud, false pretences, fraudulent personation, forging and uttering, using a false instrument and many others. Many of these laws are complex, unclear and contradictory and impede the successful investigation and prosecution of fraud, particularly that which takes place across jurisdictional borders (see Lanham 1997).

In New South Wales, the offence most directly applicable to identity-related fraud is section 184 *Crimes Act 1900* (NSW), although that section makes clear that such fraud may be prosecuted under other provisions as well. Section 184 provides:

> 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 (s. 184 *Crimes Act 1900* (NSW)).

In the other states and territories, the following offences have been used in recent years to prosecute individuals who have perpetrated acts of dishonesty involving misuse of identity.

Australian Capital Territory
Theft (s. 99 Crimes Act 1900)
Obtaining a financial advantage by deception (s. 104(1) Crimes Act 1900)
Making a false instrument (s. 135C(1) Crimes Act 1900)
Using a false instrument (s. 135C(2) Crimes Act 1900)

New South Wales
Fraudulent misappropriation (s. 178A Crimes Act 1900)
Obtaining money etc by deception (s. 178BA Crimes Act 1900)
Obtaining money by false or misleading statements (s. 178BB Crimes Act 1900)
Obtaining credit by fraud (s. 178C Crimes Act 1900)
False pretences (s. 179 Crimes Act 1900)
Fraudulent personation (s. 184 Crimes Act 1900)
Forging and uttering (s. 250 Crimes Act 1900)

Northern Territory
Stealing (s. 210 Criminal Code)
Criminal deception (s. 227 Criminal Code)
Unlawfully altering data processing material with fraudulent intent (s. 276(1) Criminal Code)

Queensland
Stealing (s. 398 Criminal Code)
Fraud (s. 408C(1) Criminal Code)
Misappropriation (s. 408C Criminal Code)
False pretences (s. 427(1) Criminal Code)
Falsifying records (s. 441(d) Criminal Code)

Producing false records (s. 441(e) Criminal Code)
Uttering (s. 489 Criminal Code)

South Australia
Fraudulent conversion (s. 184 Criminal Law Consolidation Act 1935)
False pretences (s. 195 Criminal Law Consolidation Act 1935)

Tasmania
Stealing (ss. 229(1)(b) and 234 Criminal Code Act 1924)
Dishonestly acquiring a financial advantage (s. 252A(1) Criminal Code Act 1924)
Inserting false information on data (s. 257E Criminal Code Act 1924)
Attempting to dishonestly acquire a financial advantage (s. 299 Criminal Code 1924)

Victoria
Obtaining property by deception (s. 81(1) Crimes Act 1958)
Obtaining financial advantage by deception (s. 82 Crimes Act 1958)

Western Australia
Stealing (s. 378 Criminal Code)
Stealing as a servant (s. 378(7) Criminal Code)
Fraud (s. 409(1) Criminal Code)
Forging (s. 473(1)(a) Criminal Code)
Uttering (s. 473(1)(b) Criminal Code)
Preparation for Forgery (s. 474(1) Criminal Code)
Attempted Fraud (s. 552 Criminal Code)
Conspiracy to commit fraud (s. 558(1) Criminal Code)

There is little uniformity between the various jurisdictions and it is sometimes difficult to determine which offence to use when framing charges. There are also inconsistencies in the maximum penalties that attach to similar offences in the various States and Territories.

Evaluating Commonwealth Criminal Code Reforms

In order to harmonise these laws, the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General has devised uniform laws relating to economic crime for introduction throughout Australia. The Commonwealth has recently enacted these model laws in its *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* (Cth) which commenced operation on 24 May 2001. The main Commonwealth Criminal Code Fraud Offences are:

Obtaining property by deception (s. 134.1)

where a person, by a deception, dishonestly obtains property belonging to the Commonwealth with the intention of permanently depriving the Commonwealth of the property. Maximum Penalty: Imprisonment for 10 years.

Obtaining a financial advantage by deception (s. 134.2)

where a person, by a deception, dishonestly obtains a financial advantage from the Commonwealth. Maximum Penalty: Imprisonment for 10 years.

General dishonesty (s. 135.1)

where a person does anything with the intention of dishonestly obtaining a gain from, or causing a loss to, the Commonwealth. Maximum Penalty: Imprisonment for 5 years.

Obtaining financial advantage (s. 135.2)

where a person obtains a financial advantage for himself / herself or another person from a Commonwealth entity knowing or believing that he or she is not eligible to receive that financial advantage. Maximum Penalty: Imprisonment for 12 months.

Conspiracy to defraud (s. 135.4)

where a person conspires with another person with the intention of dishonestly obtaining a gain from, or causing a loss to, the Commonwealth

The main Commonwealth Criminal Code forgery offences are:

Forgery (s. 144.1)

where a person makes a false document with intention to dishonestly induce a Commonwealth public official to accept it as genuine, or to dishonestly cause a computer, a machine or an electronic device to respond as if the document were genuine, and thereby to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function. Maximum Penalty: Imprisonment for 10 years.

Using forged document (s. 145.1)

where a person knowingly uses a false document with intention to dishonestly induce a Commonwealth public official to accept it as genuine, or to dishonestly cause a computer, a machine or an electronic device to respond as if the document were genuine, and thereby to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function. Maximum Penalty: Imprisonment for 10 years.

Falsification of documents (s. 145.4)

> where a person dishonestly damages, destroys, alters, conceals or falsifies a Commonwealth document with the intention of obtaining a gain or causing a loss. Maximum Penalty: Imprisonment for 7 years.

This legislation also amends the law governing geographical jurisdiction to facilitate the prosecution of cross-border fraudulent criminal activity.

In addition, efforts have been made to amend computer crime laws to ensure that identity-related crimes carried out electronically can be prosecuted. The Australian parliament has, for example, recently enacted the *Cybercrime Act 2001* (Cth) which commenced operation on 21 December 2001. This Act inserts a new Part into the Commonwealth *Criminal Code Act 1995* and largely follows the provisions of the Council of Europe's *Convention on Cybercrime* (2001) which was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 and opened for signature on 23 November 2001 in Budapest.

Although limited in its Commonwealth focus, the *Cybercrime Act 2001* significantly improves the scope for prosecuting cyber criminals by introducing substantive offences and procedural provisions consistent with those of the Convention. Whilst a significant improvement, there still remains some uncertainty in relation to the scope of warrants, the ability of police to intercept E-mails prior to delivery, obtaining data not on premises, extra-territorial searches and mutual assistance orders (see Ghosh 2002).

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.

Section 477.1 creates the offence of unauthorised access, modification or impairment with intent to commit a serious offence. Maximum Penalty: Not exceeding that for the serious offence.

Section 477.2 creates the offence of unauthorised modification of data to cause impairment, while s. 477.3 creates the offence of unauthorised impairment of electronic communication. Maximum Penalty: Imprisonment for 10 years (each offence).

Section 478.1 creates the offence of unauthorised access to, or modification of, restricted data (which means data held in a computer to which access is restricted by an access control system). Maximum Penalty of 2 years imprisonment.

Sections 478.3 and 478.4 relate to possession or control of data with intent to commit a computer offence, and producing, supplying or obtaining data with intent

to commit a computer offence. Maximum Penalty: Imprisonment for 3 years (each offence).

The Commonwealth *Cybercrime Act 2001* also provides new investigative powers under the *Crimes Act 1914* (Cth) and *Customs Act 1901* (Cth), allowing a magistrate to grant an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow investigating officers to: access data held in or accessible from a computer on warrant premises; copy the data; and convert data into documentary form. The penalty for failure to comply with such an order is 6 months' imprisonment.

More serious and organised fraudulent activities may also be dealt with under Commonwealth laws relating to:

• Recovery of proceeds of crime under the *Proceeds of Crime Act 1987* (Cth) (with a new *Proceeds of Crime Bill* currently before Federal Parliament including civil forfeiture provisions);

• Investigation of organised crime under the *National Crime Authority Act 1984* (Cth); and

• Conspiracy and aiding and abetting provisions under the *Crimes Act 1914* (Cth).

Reviewing the Effectiveness of a Points-based System of Identification

There are also various regulatory pieces of Commonwealth legislation that set out offences for acting dishonestly when establishing one's identity. The *Financial Transaction Reports Act 1988* (Cth), for example, regulates the manner in which identity must be established when accounts with financial institutions are created.

A 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:
- Certificate of citizenship
- Current passport
- Birth certificate

Secondary documents include:

- Driver's licence (40 points)
- Public employee or student ID card (40 points)
- Credit card (25 points)
- Medicare card (25 points)
- 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)).

• Knowingly or recklessly making a false or misleading statement in advising a financial institution of a change of name 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 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, or for alternative means of identification to be used, such as interviews, or biometrics (see Biometrics Institute 2002).

Considering the need for an Australian equivalent to the *Identity Theft and Assumption Deterrence Act* 1998 (US)

In the United States, specific legislation has been introduced to deal with identity-related crime.

The Federal *Identity Theft and Assumption Deterrence Act 1998* (18 USC 1028) which became effective on 30 October 1998, 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.

The question arises as to whether Australia, or its States and Territories should enact specific identity fraud legislation. As we have seen, there have already been substantial reforms made to relevant economic crime legislation in Australia and it may be unnecessary to enact yet another piece of legislation to deal with this type of crime. 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. Most of the problems that arise at present lie in the administration of the current regulatory controls, not with the legislation itself, although until each of the States and Territories enacts uniform legislation, problems of harmonisation remain.

The provision in the United States *Identity Theft and Assumption Deterrence Act* that enables the Federal Trade Commission to act as a clearinghouse for offences, provides a useful model that Australia could consider, however. At present, the initiative of the Australian Bureau of Criminal Intelligence, in which the Fraud Desk is being used to collate reports of identity-related fraud, has great potential and may provide an effective non-legislative solution for Australia.

Although the enactment of specific identity 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. As in other areas of fraud control, the most effective responses will probably lie in risk management and fraud prevention rather than in trying to achieve crime control through the deterrent effects of criminal prosecution and punishment.

Identifying and Countering the Practical Barriers to a Successful Prosecution

Part of the problem lies in the many practical barriers that exist to achieving a successful prosecution of identity-related fraud. The difficulties lie in encouraging victims to report these offences, in obtaining evidence, in locating offenders and arranging for their attendance at court, and in presenting evidence of sometimes complex criminal activities to courts and juries.

Many problems arise in investigating cases of identity fraud as they often involve the use of highly sophisticated techniques of deception and planning. Offenders often go to considerable lengths to make identification of themselves difficult and financial trails of evidence obscure.

Other issues which may complicate an investigation relate to the logistics of search and seizure during real time, problems of translation of non-English language evidence, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology.

Financial considerations have also meant that only the most serious cases involving substantial monetary losses are likely to be fully investigated and tried, with the attendant possibility of convicted offenders receiving the most severe sanction of a term of imprisonment. The legal response to identity fraud has, therefore, been severely restricted, although the possibility of criminal prosecution and sanction has always remained open.

Because identity fraud often does not involve face-to-face communication, 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. The perpetrators of many identity-related crimes are often not large corporations. They are able to close-down their operations quickly and easily, move assets to secure locations and use digital technologies to disguise evidence. Few remedies are available to those who fall victim to such activities. Even if one is able to mobilise the law, the chances of locating the fraudsters, obtaining extradition, mounting a prosecution, or recovering compensation may be impossible.

Even where a perpetrator has been identified, two problems arise in relation to the prosecution of offences which have an international aspect: first, the determination of where the offence occurred in order to decide which law to apply; and, secondly, obtaining evidence and ensuring that the offender can be located and tried before a

court. Both these questions raise complex legal problems of jurisdiction and extradition.

Although many of the legal and procedural impediments to the successful prosecution have been removed, a number of practical difficulties still remain. The most problematic relate to cost and delay in cases of extraterritorial law enforcement which makes some prosecutions practically impossible. Moreover, cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities across nations which, despite prevailing trends towards globalisation, exists only infrequently.

There are also numerous problems associated with conducting criminal trials in cases involving identity fraud. The principal difficulties relate to the presentation of computerised business and accounting records to a court, the difficulty of presenting complex financial transactions to a jury in such a way as to permit lay people, perhaps unfamiliar with the technologies used, to understand the factual issues involved, and the length of time which such trials take, which is often exacerbated in cases of criminal conspiracy by having multiple defendants and multiple charges.

Various reforms to court procedures have been introduced, however, in recent years to reduce the length, complexity, and cost of prosecutions, particularly those which involve substantial sums of money or complex factual circumstances. Computer technology, for example, has greatly facilitated the presentation and analysis of complex business dealings in some courts. In addition, legal practitioners are often closely regulated with respect to the length, manner and nature of material which they present to the courts.

In view of the complexities associated with the conduct of criminal trials involving allegations of identity fraud, it is necessary for all those involved to be thoroughly trained in carrying out their various duties in an efficient and effective way. Witnesses, particularly forensic accountants, need to be trained in the presentation of technical information to courts and juries in much the same way as expert medical witnesses have specialised in presenting complex medical testimony in clear and simple terms to courts. Legal practitioners also need to be trained not only in the particular evidentiary and procedural rules which apply in such cases, but in liaising effectively with accountants and financial advisers, particularly when presenting lengthy and complex financial records. Just as specialist groups of lawyers now exist for dealing with such cases, so a specialist Judiciary needs to be established in order to ensure that judges with appropriate experience and financial and information technology skills are allocated to these trials. Finally, jurors and those lay witnesses who give evidence in such cases should be provided

with information which will enable them to understand the latest court procedures and arrive at decisions in an efficient manner.

In terms of procedural reform, a number of improvements have been suggested. These include taking early steps to ensure that evidence and facts are agreed and admitted wherever possible; streamlining interviewing procedures and using teleconferencing technologies for interviewing; using documentary evidence in preference to oral testimony wherever possible; overcoming the barriers to the use of computer-generated evidence; ensuring that evidence is not altered or destroyed before it is able to be obtained from another country; ensuring that police have access to the plain text version of encrypted files, either by requiring the suspect to disclose the encryption key, or by employing trusted third parties to hold copies of private encryption keys which can then be used by law enforcement on production of a warrant.

Information networks within and between law enforcement agencies also need to be used, so that when an investigation begins, contact can be made immediately with the appropriate person in another country's corresponding department. Secure Intranets, such as that used by the Australian Bureau of Criminal Intelligence, are an excellent way in which this can be achieved. They can also be used to share 'Fraud Alert' information and to exchange intelligence needed in investigations.

Twenty-four hour response centres are now being established in many countries. These centres, which are to be used for genuine emergencies only, enable requests for real-time computer investigations to be handled at any time of the day or night in the participating country. In Australia, the Australian Federal Police handles such requests and refers queries to relevant state and territory police services of other Australian Federal Police regional offices (Geurts 2000).

Conclusions

Identity fraud has created considerable problems for law enforcement and regulatory agencies globally in recent years. In part, the problems are not essentially different from in the past, as offenders have used fraudulent misrepresentation for hundreds of years to commit crime. The advent of digital technologies has, however, had the effect of making such conduct easier to commit and more difficult to detect. Because many offences are committed across jurisdictional borders, it is also considerably more difficult to mount a prosecution than in the past.

Australia's legislative package to deal with crimes of this nature is comprehensive and rarely have offenders been able to escape conviction simply because of the absence of appropriate criminal offences with which to charge them.

The practical problems of actually conducting an effective investigation, prosecution, and trial are, however, considerable and it is here that the legal system breaks down.

The two solutions of harmonisation of laws and sharing of information through cooperative effort both need to be addressed.

In the end, however, governments need to establish policies to maximise the chances of offenders who manipulate proof of identity documents being detected. Coupled with sensible self-help precautions, this will provide more practical benefits than seeking to deter this kind of conduct through criminal justice responses.

References

Australasian Centre for Policing Research 2000, *The Virtual Horizon: Meeting the Law Enforcement Challenges*, Scoping Paper, Australasian Centre for Policing Research, Adelaide.

Australian Federal Police 2001, 'Identity Fraud Trends', *Comfraud Bulletin*, No 23, pp. 1-3. http://www.afp.gov.au/page.asp?ref=/Crime/Fraud/ComfraudBulletins.xml.

Bennett, J. 2002, 'Identity Fraud: Getting Inside the Criminal Mind', National Crime Authority Source: http://www.nca.gov.au/html/pg_spchs.htm).

Biometrics Institute 2002, 'Biometric Technologies'. http://www.biometricsinstitute.org/bi/types.htm (visited 29 May 2002).

Council of Europe 2001, *Convention on Cybercrime*, European Treaty Series No 185, Budapest, 23 November 2001, Council of Europe, Strasbourg (http://conventions.coe.int/treaty/EN/projets/projets.htm)

Ellison, L. 2001, 'Cyberstalking: Tackling Harassment on the Internet, in Wall, D. S. (ed.), *Crime and the Internet*, pp. 141-51, Routledge, London.

Forde, P. and Armstrong, H. 2002, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, 16-18 July, Sherwell Conference Centre, University of Plymouth, Plymouth. http://www.cbs.curtin.edu.au/Workingpapers/other/Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20Criminals.doc (visited 29 May 2002).

Geurts, J. 2000, 'The Role of the Australian Federal Police in the Investigation of High-Tech Crimes', *Platypus Magazine: The Journal of the Australian Federal Police*, March, http://www.afp.gov.au/publica/platypus/mar00/intfrd.htm (visited 5 February 2001).

Ghosh, A. 2002, 'The Cybercrime Act 2001: Implementing the European Union's Cybercrime Convention', Paper presented at the RSA Conference, San Jose, 16-22 February.

Health Insurance Commission 1997, *Annual Report 1997-98*, Professional Review Supplement, Australian Government Publishing Service, Canberra.

Lanham, D. 1997, *Cross-border Criminal Law*, John Libbey & Co, Sydney.

McKinnon, M. 2002, 'Boatpeople ID Scam', *Courier Mail (Brisbane)*, 15 February.

McLellan, D. 2001, 'Ex-Centrelink Staffer Pleads Guilty of Fraud', *Canberra Times*, 28 November, p. 5.

Securities and Exchange Commission 2002, 'Regulators Launch Fake Scam Web Sites to Warn Investors About Fraud'. http://www.sec.gov/news/press/2002-18.txt (visited 29 May 2002).

Smith, R. G., Holmes, M. N. and Kaufmann, P. 1999, 'Nigerian Advance Fee Fraud', in *Trends and Issues in Crime and Criminal Justice*, No. 121, Australian Institute of Criminology, Canberra.

Smith, R. G. and Urbas, G. 2001, *Controlling Fraud on the Internet: A CAPA Perspective. A Report for the Confederation of Asian and Pacific Accountants*, Research and Public Policy Series No. 39, Confederation of Asian and Pacific Accountants, Kuala Lumpur / Australian Institute of Criminology, Canberra.

Warton, A. 1999, 'Electronic Benefit Transfer Fraud: The Challenge for Federal Law Enforcement', *Platypus Magazine: The Journal of the Australian Federal Police*, No. 65, December, pp. 38-44.