AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 129

Identity-related Economic Crime: Risks and Countermeasures

Russell G. Smith

In dealing with government agencies and in conducting many business transactions, people are required to establish who they are by providing evidence of some unique identifying characteristics. Even using a key to open a door is a means of ensuring that a specified individual is able to gain access although, of course, a key may be stolen or used by someone other than the intended holder. In the past, identity was more easily verifiable as people conducted most of their transactions in person. Since the development of electronic communications technologies, however, we can no longer be certain that the person at the end of a fibre optic cable is who they claim to be. The difficulty in establishing a person's identity with certainty is a boon to criminals, as they are able to fabricate documents which may be used to misrepresent their identity, then commit a crime and ensure that they cannot be located. This paper examines the nature of such deception and the innovative ways in which it is being addressed through the use of modern technologies.

Adam Graycar
Director

People are required to provide evidence of their identity for a wide range of purposes when dealing with governments or transacting business. When we obtain a driver's licence, a tax file number or a Medicare card, or open an account with a bank or shop, we need to refer to a range of personal details in order to establish who we are and where we live. In addition, when we log on to a computer, use a plastic card in an automated teller machine or conduct an EFTPOS transaction, we have to establish our identity through the use of a password or personal identification number (PIN).

In the future, in order to pay for goods and services purchased via the Internet, we will have to obtain a cryptographic key pair for use in a public key computer system. To obtain this key pair, we will need to provide sufficient evidence of our identity to the issuing authority. Identifying ourselves, therefore, will become an integral part of everyday life. Those people, such as the homeless or illegal immigrants, who are unable to produce satisfactory evidence to confirm their background and where they live, may be unable to use many of the services which others take for granted.

One of the most frequently used strategies to perpetrate fraud is the creation of false documents used to misrepresent one's identity. Once a convincing identity has been fraudulently established, it is then possible to steal money or otherwise to act illegally and then to evade detection, investigation and arrest. Australian police services have recently found an increase in such misrepresentations which have been used for money laundering and tax evasion, to obtain personal loans from banks, enter into hire-

September 1999

ISSN 0817-8542
ISBN 0 642 24126 0

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

purchase agreements, and deal in stolen motor vehicles (Wahlert 1998). Often, counterfeit documents have been created by a single person to support multiple identities, each used only once for a specific illegal enterprise and then discarded. The objective in each case is to obtain a benefit without leaving evidence to connect the offender to the crime in question.

In the past, the forgery of documents that were used to provide evidence of identity was a highly skilled task that few criminals were able to undertake convincingly. Since the advent of digital technologies, however, it is much easier to scan an official document electronically, alter the image as it appears on a screen, and print out a counterfeit version using high quality laser colour printers—all from the comfort of a home office.

Official statistics have not been gathered on the extent to which fraud is carried out in this way. However, recent business victimisation surveys have indicated that fictitious identities are being used to perpetrate a variety of offences and that the problem is perceived as being an important security risk within organisations.

In February 1999, KPMG carried out a survey of over 1800 of Australia's largest businesses. Of the 367 replies received, some 7280 incidents of fraud were reported in the two years preceding the survey, with 57 per cent of respondents reporting at least one incident during that period. Of the incidents committed by managers, 9.6 per cent involved the use of false documentation. Of the incidents committed by persons outside organisations, 11.9 per cent involved the use of false documentation and 13.7 per cent related to forgery of cheques (KPMG 1999).

In surveys of computer crime and security incidents conducted by the Victoria Police and others in 1997 and 1998, 15 per cent and 19 per cent, respectively, of the organisations surveyed, thought that identity-related fraud would have an impact on their organisation over the next five years (OSCA and Victoria Police 1997; Victoria Police and Deloitte Touche Tohmatsu 1999).

In the United States in 1997, the Secret Service made nearly 9500 arrests in which so-called identity theft was an issue, amounting to US$745 million in losses to individual victims and financial institutions. It has been estimated that 95 per cent of financial crimes in the United States involve stolen identities, with financial losses in respect of such crime nearly doubling in the two years preceding 1998 (Kyl 1998). In an attempt to improve knowledge of the extent of identity-related fraud, the Identity Theft and Assumption Deterrence Act 1998 (Title 18 USC 1028), which makes theft of an identity a felony in the United States, requires the Federal Trade Commission to maintain a record of stolen identity reports.

Establishing an Identity for Illegal Purposes

The first step in perpetrating many acts of dishonesty is to ensure that any financial reward obtained is unable to be linked with the offender. Opening an account with a financial institution in a false name is one way in which this may be achieved. In order to prevent such conduct, the Financial Transaction Reports Regulations (Cwlth) require that sufficient evidence be produced at the time an account is opened to ensure that the customer may be located should any default later occur. There are also substantial penalties which apply where accounts are opened in a name other than that which the person usually uses.

Documentary evidence is required in the form of primary documents (such as a birth certificate, current passport or certificate of citizenship—each of which carries 70 points) and secondary documents (such as a driver's licence, public employee or student identification card—each worth 40 points—or a credit card, Medicare card or council rates notice—each worth 25 points). A variety of other documents may be used to verify one's name and address, each carrying differing 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 (OGIT 1998).

Reliance on this system does not, however, provide a complete solution to the problem as it is possible to submit documents that have been forged or altered, often through the use of computerised desktop publishing equipment.

In Victoria, for example, between August 1995 and March 1996, an offender used desktop publishing equipment to create 41 birth certificates and 41 student identification cards (some containing photographs), each in separate names, and a counterfeit driver's licence. These were used to open 42 separate bank accounts throughout the Melbourne metropolitan region to pay cheques into accounts as wages and make immediate withdrawals before they had cleared; to register a business name; to obtain sales tax refunds; and to defraud various retailers. The offender was charged with a variety of State and federal offences and sentenced to five years' imprisonment with a non-parole period of three years. He was also ordered to pay compensation of $41,300 and reparation to the Commonwealth of $458,383 (R v *Zehir*, Court of Appeal, Supreme Court of Victoria, 1 December 1998).

The Federal Government's *Project Gatekeeper* has proposed that key pairs to be used in the Public Key Technology

Framework would be issued to individuals who are able to establish their identity to an appropriate degree of assurance by supplying multiple and independent sources of identification, such as those referred to above (OGIT 1998). The principal means by which fraud could be carried out in such a system would be for offenders to submit false documents to registration authorities in order to have cryptographic key pairs issued to them for use in fraudulent ways.

Alternatively, there is the possibility that key tokens, which would take the form of smartcards, could be stolen and used without authorisation by compromising their security features. Illegal access could also be gained to cryptographic keys that would be stored on personal computers or servers.

The adoption of appropriate risk management measures would help to reduce the likelihood of such abuses taking place. It would be necessary for registration authorities to adopt appropriate standards and procedures in order to verify the documents relied upon by people to establish their identity when key pairs are issued.

Countermeasures

There are four primary methods that may be used to authenticate a person's identity (although there is some overlap between the following categories). Generally, these are based on:

- **something that you have**, such as a key or a plastic card (tokens);
- **something that you know**, such as a password or date of birth (knowledge);
- **something related to who you are**, such as your appearance, signature, or fingerprint (biometrics); or
- **something indicating where you are located**, such as your address and a corresponding telephone number (location).

There are, of course, others, such as the use of a person's name, and a variety of behavioural and psychological characteristics which are able to be used to identify someone (see Clarke 1994).

Effective fraud prevention strategies have been devised which target each of these four aspects. Depending upon the degree of confidence with which a person's identity must be established, it is possible to make use of one or more of these four methods. Each, however, has its own vulnerabilities that are able to be exploited by those who want to act illegally.

Token Security

An extensive range of security measures have been devised to ensure that documents (such as cheques, banknotes and passports) and devices (such as keys and plastic cards) are hard to counterfeit or to alter.

Standard paper documentary security features include the use of:

- laid lines, which are printed lines spaced unevenly to prevent documents being cut and pasted together;
- colour prismatic printing, which is unable to be scanned or photocopied;
- void pantographs, which disclose the word "void" when they are copied;
- warning bands, which explain the security features that are built into documents;
- high-resolution borders, which are intricate and difficult to reproduce designs printed on the borders of documents;
- holograms or multi-colour three-dimensional images;
- micro-printing, in which words or phrases are only able to be read if magnified;
- secure number fonts, which have numbers embedded with matching words;
- artificial watermarks; and
- chemical voids, in which the word "void" appears when certain chemicals are used to remove ink from the document.

Some documents, such as passports, are also now being digitally created with enhanced levels of security.

Plastic cards may be protected through the use of:

- matching account numbers on the front and back of the card;
- micro-printing;
- holograms;
- embossed characters and numbers;
- tamper-evident signature panels;
- magnetic stripes with improved card validation technologies;
- special inks which show words or symbols only under ultraviolet light; and
- optical variable devices such as exist on some banknotes.

Smartcards, of course, are much more difficult to counterfeit or alter than ordinary magnetic stripe cards by reason of the need to re-engineer the silicone chip used to record data on the card. It has been found, however, that the encryption used on smartcards can be broken if certain types of errors can be created on the card, such as through the use of ionising or microwave radiation. For example, Bellcore, a United States computer and communications security company, and others have identified a number of design flaws in computer chip cards which may permit data to be leaked or information contained in the card to be tampered with (see Denning 1998). A more simple problem with smartcards, of course, is that access to the card is usually only protected by a PIN.

Another means of reducing the risk of counterfeiting is to impose controls on the availability of the raw materials used in the manufacture of counterfeit cards and documents—namely, white plastic and paper. In Canada, the RCMP introduced a campaign of issuing warning posters to companies which design and distribute white plastic and embossing machines used in the production of credit cards. The companies used the notices to educate staff about security and to monitor unusual requests for materials that could be used for counterfeiting (Duncan 1996).

The main problem with relying upon the use of such an extensive range of security features is that those who are required to validate documents might not be familiar with all of the features present in the legitimate document and not trained to recognise counterfeit or altered copies. Staff who are presented with documents used to provide evidence of one's identity should not only be trained to recognise counterfeit documents but should also be required to validate the documents relied upon with the issuing source. Staff presented with a birth certificate should, for example, check if the details correspond with those held in the central office of Births, Deaths and Marriages. An electricity account tendered in support of one's identity should be validated by checking with the electricity company concerned.

This may not always solve the problem, however, as telephone answering services can be manipulated to support fabricated employment or personal details. Sometimes, offenders create phantom businesses in a rented office with an answering machine and a fax expressly for the purpose of circumventing documentary checks. There is also the possibility of staff being subjected to intimidation or violence if they refuse to accept documents or process transactions, or delay unduly.

Knowledge-based Security Systems

Any security system which makes use of information known only to a given individual may be compromised if that information is able to be discovered through illegitimate means. Passwords and PINs used as a means of restricting access to computer systems are popular at present, although frequently misused and abused (see Denning 1999). It is possible to guess passwords, particularly if little or no thought has been given to their selection, or to use various forms of social engineering to trick users into revealing their passwords for subsequent improper use.

Users are often neglectful when dealing with PINs and passwords. Despite continual publicity of the need to protect plastic card PINs, cardholders continue to write them on cards or keep them with their cards, even though this may result in their being held personally liable for fraud carried out when cards are lost or stolen.

The use of brute computing force has also been used to break passwords. Password cracking programs are available by which computers are able to search entire dictionaries systematically for a password (Denning 1999, pp. 211–13). Even if passwords are encrypted so as to protect them from direct exposure, it is possible to break encryption keys through the use of massive computing resources achieved by linking numerous computers, sometimes in different countries, operating continuously for many months. In 1994, a 129-digit RSA key was broken in this way (Denning 1998, p. 40) while in August 1999, a 512-digit RSA key was compromised (Robinson 1999).

There are various ways of enhancing access security through the use of passwords (see Alexander 1995). Appropriate education of users is the first step—information can be provided on ways of ensuring that passwords are not disclosed, guessed or otherwise compromised by the user in question. Systems should be used which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Terminals should have automatic shutdown facilities when they have not been used for specified periods, such as five minutes, following which the user is required to log-on once again. Single use passwords, where the password changes with every successive log-on according to an agreed protocol known to the user and system operator, could also be used. The SecureID card, for example, every 60 seconds generates a new password that is a function of the time and a secret 64-bit seed that it unique to the card (Denning 1998, p. 44).

Challenge–response protocols may also be used as a means of carrying out user authentication. The server generates a random number that is sent to the card. In a public key system, the card digitally signs the number and returns it to the server. The server then validates the digital signature. Alternatively, call-back devices may be used. After the user dials into a computer through a modem and provides a password, the system disconnects the user and then telephones the user on a number previously registered with the server. After the user is verified, the transaction can then proceed. Such a system is, however, able to be overcome through the use of call-forwarding arrange-ments (Denning 1998, p. 45).

Biometric Security

A variety of human characteristics may be relied upon in order to provide evidence of one's identity, with the most recent technical discoveries enabling people to be identified with a very high degree of confidence. Biometric identifiers may relate to a person's physical characteristics (such as their fingerprints, DNA, retinal appearance, facial and hand geometry or even body odours), biodynamics (such as their handwriting style, signature or typing patterns) or aspects of their social behaviour (such as patterns of movement or speech) (Johnson 1996). Systems that make use of these identifiers are now being used by a range of public and private sector organisations.

One company, Fingerscan, has supplied fingerprint identification systems to Woolworths in Australia and a major Indonesian bank, both of which will use the system to replace password identification (Security Australia 1996). Two Canberra hospitals, the National Capital Private Hospital and the Canberra Hospital, are also conducting trials of systems which enable doctors to gain access to computerised patient records databases by having their fingerprints scanned electronically (Nursing Review 1998).

In Connecticut, in the United States, fingerprint scanners were introduced in 1996 in order to prevent social security fraud. Recipients of welfare cheques were required to undergo fingerprint scanning prior to collection of their payments. The introduction of the technology cost US$5.1 million, but is said to have saved the state US$9 million in fraudulent claims (Denning 1999, p. 324).

In California a company, Identix, has developed a system which has fingerprint recognition sensors on mobile telephones, computer keyboards and plastic cards (Young 1999), while the Bank of Texas has recently introduced iris recognition systems for its ATM network.

Reliance on biometric systems does, however, raise a number of practical and ethical concerns. The costs, and volume of data that must be stored online to enable comparison for any potential user, may be prohibitive and there is always the possibility that computer security systems could be compromised by reproducing data streams which correspond with the biometric characteristics in question.

An additional problem is that users are required to provide samples of their characteristic and that the security of these samples could be compromised. Some people also find the process of providing personal information in public distasteful or they believe, for example, that having one's iris scanned might be dangerous. One recent cheque fraud prevention initiative which required customers to leave their fingerprint on cheques before the cheques would be accepted by retailers was discontinued because customers were simply reluctant to use it (Pidco 1996).

Location-based Security Systems

Another system makes use of space geodetic methods to authenticate the physical locations of users, network nodes and documents. One company, CyberLocator, makes use of a location signature sensor that relies on signals transmitted by satellite to provide a location on Earth at any given time. Users can thus be located at the time they attempt to gain access to the system, which provides a safeguard against individuals pretending to be legitimate users but who are in a different physical location (Denning 1998, p. 45; Denning 1999, pp. 341–3). Such systems are mainly of use in preventing computer based fraud which is carried out by individuals located in foreign countries, who try to disguise their identity through the use of anonymous remailing technologies. For example, an offender may operate a fraudulent telemarketing operation originating from the United States, but which appears to emanate from England. Once funds have been obtained from the victim (perhaps located in Australia) it may be impossible to determine exactly where the offender is, unless the computer terminal itself can be identified geographically on the globe at the time the fraudulent acts occurred.

Maintenance of Identity Databases

Maintaining extensive databases of personal information about individuals is another way of being able to improve the validation of identities. Although this may be an effective fraud control measure, it raises considerable problems relating to privacy and the security of information being held. In the United Kingdom, for example, a long and bitter struggle surrounded proposals to introduce a voluntary national system of identity cards used in conjunction with photographic drivers' licences (Gill 1997).

In Australia in the early 1990s, the Parallel Data-matching Program was created by the Federal Government in an attempt to prevent taxation and social security fraud. This system seeks to identify individuals who have made claims for benefits to which they are not entitled, and also individuals who have not made claims to which they are entitled. In 1996–97, the program was said to have enabled direct savings of $157 million for two departments—Social Security and Employment, Education, Training and Youth Affairs. The cost of conducting the program for the same year was said to have been $25 million, resulting in a net saving of $132 million (Centrelink 1997).

The Data-matching Program has not, however, been free from criticism. This has related to the compilation of personal data by a number of government agencies, the accuracy of the cost-benefit analyses used to justify the program, and mistakes in matching which have resulted in some individuals wrongly being identified as having improperly received government payments (Birmingham 1995; Clarke 1993).

In the private sector, one example of a computerised personal identification strategy is that used by a New York retail chain, Tops Appliance City Inc. This strategy, which was introduced in 1993, involves a computer network which checks credit card applications by digitally photographing the applicant and by recording the applicant's signature and other identifying information, such as driver's licence, telephone and social security numbers. This information is then used to validate future purchases and also when the customer collects merchandise. The strategy resulted in a 90 per cent reduction in credit card fraud losses over the 17-month period following its introduction, with a 57 per cent reduction in losses per incident (Masuda 1996).

Conclusions

The steps that can be taken to prevent fraud arising from misrepresentations of identity depend upon a range of considerations:

- the likelihood that the risk will be realised;
- the cost of the countermeasures;
- the effectiveness of the technologies used;
- the user-friendliness of systems;
- privacy concerns if databases are used; and
- the possible negative consequences on the behaviour of users.

It might be possible to prevent all such forms of illegality, but the solutions may simply be too costly, unwieldy and authoritarian to be acceptable. In certain high-risk areas, however, greater precautions need to be taken to check the validity of documents relied on, or other more secure forms of personal identification need to be used. In the future, biometric systems used in conjunction with plastic cards and computers may provide more secure solutions, although adequate steps will be necessary to ensure that individual privacy is not compromised and that systems are not used for improper and inappropriate purposes.

References

Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York.

Birmingham, J. 1995, "Nowhere to hide", *Independent Monthly*, June, pp. 45-7.

Centrelink 1997, *Data-matching Program: Report on Progress 1996-97*, Centrelink, Data-matching Agency, Department of Social Security and Department of Employment, Education, Training and Youth Affairs, Canberra.

Clarke, R. 1993, "Matches played under Rafferty's Rules: The parallel data-matching program is not only privacy-invasive but economically unjustifiable as well", at: http://www.anu.edu.au/people/Roger.Clarke/DV/PaperMatchPDMP.html (visited August 1999)

Clarke, R. 1994, "Human identification in information systems: Management challenges and public policy issues", at: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html (visited August 1999)

Denning, D. 1998, "Cyberspace attacks and countermeasures", in *Internet Beseiged: Countering Cyberspace Scofflaws*, eds D. E. Denning & P. J. Denning, ACM Press, New York, pp. 29-55.

Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, Reading, Massachusetts.

Duncan, M. D. G. 1996, "Counterfeiting in a technological society", *International Criminal Police Review*, no. 456, pp. 18-21.

Gill, M. 1997, "Ethnic minorities and policing: The impact of national ID cards", *Security Gazette*, vol. 39, no. 8, p. 33.

Johnson, E. 1996, "Body of evidence: How biometric technology could help in the fight against crime", *Crime Prevention News*, December, pp. 17-19.

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

Kyl, J. 1998, "Section 512, Identity Theft", Senate Judiciary Subcommittee on Terrorism and Technology: Opening Statement, 20 May, at: http://www.senate.gov/~kyl/sidtft.htm (visited 31 August 1999)

Masuda, B. 1996, "An alternative approach to the credit card fraud problem", *Security Journal*, vol. 7, pp. 15-21.

Nursing Review 1998, "Fingerprints open records", vol. 3, no. 10, p. 14.

Office of Government Information Technology (OGIT) 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, Australian Government Publishing Service, Canberra.

Office of Strategic Crime Assessments (OSCA) and Victoria Police 1997, *Computer Crime and Security Survey*, Attorney-General's Department, Canberra.

Pidco, G. W. 1996, "Check print: A discussion of a crime prevention initiative that failed", *Security Journal*, vol. 7, pp. 37-40.

Robinson, S. 1999, "Researchers demonstrate computer code can be broken", *New York Times*, 27 August.

Security Australia 1996, "Fingerscan's $2.5m deal", vol. 16, no. 10, p. 2.

Victoria Police and Deloitte Touche Tohmatsu 1999, *Computer Crime and Security Survey*, Victoria Police Computer Crime Squad and Deloitte Touche Tohmatsu, Melbourne.

Wahlert, G. 1998, "Crime in cyberspace: Trends in computer crime in Australia", *Platypus Magazine*, no. 59, pp. 3-9.

Young, S. 1999, "Thumbs up for fingerprint-based IDs", *Age* (Melbourne), 1 June, p. IT2-4.

Acknowledgment

This paper makes use of a number of helpful suggestions offered by Dr Roger Clarke.

Dr Russell G. Smith is a Senior Research Analyst at the Australian Institute of Criminology.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.