FRAUD IN E-GOVERNMENT TRANSACTIONS: RISKS AND REMEDIES

Milind Sathye*, Eugene Clark# and Anni Dugdale**

Synopsis

As governments the world over increasingly deliver services electronically they have to face the risk of possible fraud. This paper identifies five categories of fraud in e-government transactions and the three recognised ways of dealing with it. Further, it discusses the legal remedies presently in place to combat e-fraud, and places Australian regulatory solutions within the broader context of international regulations. Finally, the paper offers some possible options which, inter alia, include legislating an Australia-wide anti-identity theft regime, establishment of a National Vigilance Commission, protection and reward for whistle blowers, and identity fraud awareness campaigns to combat the menace of e-fraud.

* Associate Professor, School of Business and Government, Division of Business, Law and Information Systems, University of Canberra, Master of Commerce (Accounting and Finance), Ph D (Finance and Banking).

Professor, School of Law, Division of Business, Law and Information Systems, University of Canberra, PhD, JD(Hons), MEd Studies, MEd, BA.

** Senior Lecturer, Sociology, University of Canberra, BSc(Adel); Dip Ed (Adel); MA (UNSW); PhD (Wollongong - STS).

Background

Governments the world over are increasingly delivering services electronically as this has been found to be cost effective and efficient. However, electronic delivery of services is a double-edged sword. On one hand, electronic delivery of services brings benefits; yet on the other, the same electronic medium creates enormous opportunities for economic offenders. Hacker attacks, e-mail defamation, intellectual property losses, loss of data due to electrical failures, computer viruses, computer fraud, occupational health and safety, privacy, and new requirements for people with disabilities are just a few of the challenges facing today's organisations, both public and private (Grabosky, Smith & Dempsey 2001).

Fraud is one of the fastest growing crimes in Australia. The e-transaction context, with identities often disguised, further compounds the situation. According to the Australian Institute of Criminology, the estimated cost of fraud to Australia is $5.88 billion a year, which represents almost a third of the total cost of crime in Australia. Identity fraud, in particular, poses a significant financial cost to the community with estimates ranging from $2 billion to $3.5 billion a year (Australian Institute of Criminology, 2003). The federal Attorney-General's Department has defined fraud as 'dishonestly obtaining a benefit by deception or other means' (Attorney-General's Department 2002, p. 4).

The enormity of the problem of fraud, in particular e-fraud, has been recognised at the national level. 'The [Australian] Government views fraud as an issue that has priority and ought to be dealt with in a coordinated manner at the national level' (Attorney-General's Department 2000). A joint report of the Australian Institute of Criminology and PricewaterhouseCoopers (2003) states that computer-based financial crimes have 'the capacity to retard legitimate business development … and security risks have slowed the implementation of online business models'. The Hawker Committee (2001) recognised the gravity when it stated that '... identity fraud is a significant issue for the Australian community'. There have been long debates on sensitivities that surround the establishment of identities. For example, in the mid 1980s, the federal government developed a proposal for a national identification scheme (Australia Card). However, due to public concern about the scheme's privacy implications, the Bill was defeated (Clarke 1987). As Australian governments move towards full e-government, they will increasingly need to confront and find solutions for many of the same e-fraud problems that e-businesses are currently facing.

Exposure to fraud risk in e-transactions

Major ways in which e-fraud may be committed have been enumerated by Smith (2000). Relevant to e-fraud are:

- **Fraud involving paper-based payment systems**: A fraudster can open a bank account with false identity and issue cheques in excess of the credit balance in the account to obtain online goods or services. If the business or government agency providing the service does not wait for authentication checks to be carried out, it may expose itself to fraud risk.
- **Fraud involving direct debit system**: If the agency providing the service does not wait until funds are actually received to its account, it may expose itself to risk. This can happen where online payments are made by direct debit to a payer's account and credited to the recipient's bank.
- **Fraud involving electronic funds transfer**: It is possible for private encryption keys to be stolen or used without authorisation. This can be done by submitting false identification to obtain the public–private key pair. If the private key is held on a smart card, the access control device (for example, a password) could be broken to obtain the key. This would enable unauthorised people to order goods and services online.

- **Identity fraud**: Users can disguise their identities whilst online. Consumers of government services will need to be confident they are dealing with the legitimate government agency. In online transactions, the user needs to be sure the provider is genuine and providers need to be sure that legitimate users are making use of services.

E-fraud in government transactions in Australia

Studies on e-fraud so far relate mainly to businesses. As government departments are increasingly offering the facility of e-transactions, these departments have also become vulnerable to e-frauds. The Australian National Audit Office, in its survey of fraud in the public service, indicates that agencies reported experiencing a total of $1.69 million in internal fraud in 2000–01 and $2.63 million in 2001–02. Agencies reported a total of $115.13 million in external fraud in 2000–01 and $90.7 million in 2001–02 (Australian National Audit Office 2003, p.3).

The Klumzeld Peat Marwick Goerdeler survey on fraud found that 62 per cent of 39 government organisations surveyed had experienced fraud (KPMG 1999, p. 13.). Smith (1999) classifies fraud in e-government transaction into five categories. These, in descending order of financial losses, are:

- theft of benefits
- misappropriation of funds
- stealing information
- stealing computer hardware and software
- misuse of time.

Theft of benefits

Revenue fraud includes attempts to disguise transactions in order to avoid payment of tax. In addition, attempts can be made to manipulate payment of refunds or to increase entitlements to benefits. For example, in 2002, a Queensland businessman was found guilty of GST refund related fraud and was ordered to repay $104 852 to the tax office (Australian Taxation Office 2002).

Social security and health benefit fraud: The ANAO (2003, p. 3) reported that 'the most frequent form of external fraud reported in the 2002 survey was fraudulent claims for Commonwealth benefits and payments'. This form of fraud also had the greatest dollar value attributed to it, $28 million in 2000–01 and $42 million in 2001–02. The recent Snowtown serial murders in Australia is an example of identity fraud; social security payments continued to be paid to some of the victims' accounts even after their death (Standing Committee on Economics, Finance and Public Administration 2000, p. 12).

Credit card fraud: Government credit cards can be misused and funds misappropriated through unauthorised use. The problem is so serious that the Office of the Minister for Justice has appointed a joint committee of representatives of the banking industry and the Australian Government to tackle such fraud (Minister for Justice and Customs 2003).

Misappropriation of funds

Cases of misappropriation of government funds continue to be reported. Recently, a Deloitte Touche and Tohamatsu audit found that $927 148 was unaccounted for by the Western Australian Aboriginal Community Controlled Health Organisation (McGinty 2003). Poor government management of risks associated with purchasing services from non-government organisations contributes to such lack of accountability for expenditures (Auditor General for Western Australia 2003).

Stealing information

Smith (1999) states that the greatest risk lies in government-owned software being downloaded and used on personal computers for private purposes. The House of Representatives Standing Committee on Economics, Finance and Public Administration(2000) found there were excess tax file numbers, many of which were used to commit fraud.

Stealing computer hardware and software

Computer equipment, which may have valuable software installed; and may contain sensitive information, may also be stolen. In 2003, for example, two computers were stolen from Australian Customs Office. It was initially believed the computers contained sensitive information, however, the government later confirmed that they did not (Ellison 2003).

Misuse of time

Instead of using office time for doing legitimate office work, employees may carry out personal work, resulting in loss of productivity. For example, 'in December 2000, five police officers were dismissed after widespread use of the New South Wales Police Service email system to disseminate pornographic and violent material' (Dixon 2001). In order to combat such problems, businesses and government departments use a variety of methods. Some of the strategies commonly used are described in the next section.

Strategies to deal with e-fraud

As Smith (2000) stated, three generally recognised ways of dealing with e-fraud exist. The first is legislation, that is, enacting suitable laws, also called 'hard regulations'; secondly, soft regulations like codes of practice; and lastly, preventive strategies to combat fraud.

Regulations in Australia

Hard regulations in Australia comprise:

- **Civil action**: Commonwealth and state laws are generally in place, which give a right to rescind the contract or sue for damages where misleading or deceptive advertisements are placed on the Internet.
- **Consumer protection**: Consumer protection laws are designed to ensure consumers are not coerced into buying products they do not want, and are not otherwise deceived by sellers.
- **Criminal action**: Criminal prosecution acts as a deterrent to perpetrators of fraud. Besides fines and imprisonment, adverse publicity, professional disciplinary sanctions, civil action, injunction orders and the like also act as deterrents.

The most significant development in this area is the passage of the *Cybercrime Act 2001* (Cwth) on 27 September 2001. This Act amended the *Criminal Code Act 1995* (Cwth) through addition of new computer offences that were based on the January 2001 Model Criminal Code Damage and Computer Offences Reported, developed through federal, state and territory cooperation. The new Act also repealed existing offences in Pt VIA of the *Crimes Act 1914* (Cwth) that was enacted in 1989 and predated existing technologies. The Cybercrime Act provides for enhanced investigation powers relating to the search and seizure of electronically-stored data, by amending the Crimes Act and the *Customs Act 1901* (Cwth).

Under the Cybercrime Act, new offences include:

- access or modification of computer data and impairment of electronic communications
- unauthorised modification of data – would catch a person who is reckless as to whether their actions will impair data, for example, circulation of a virus

- unauthorised impairment of electronic communications, for example, denial of service attack
- unauthorised access or modification of restricted data, for example, giving password to an unathorised person
- unauthorised impairment of data on a federal computer disk or credit card
- possession or control of data with intent to commit a computer offence
- producing, supplying or obtaining data with intent to commit a computer offence – targeted at a situation where preparatory action is taken but the intended offence is not completed.

The new legislation includes offences that carry penalties of up to 10 years and cover:

- hacking
- distribution of viruses
- denial of service attacks
- unauthorised access with intent to commit a serious offence
- misuse of a limited authority, eg an employee using limited access rights to enter the system and fraudulently transfer funds
- development, supply or possession of viruses or hacking programs.

The Cybercrime Act has a wide jurisdiction and covers offences where the conduct constituting an offence occurs partly in Australia; where conduct occurs on board an Australian ship or aircraft; and where the person committing the offence is an Australian citizen or an Australian company.

One of the most controversial aspects of the Act is its expanded powers of investigation. These include allowing a magistrate to make an assistance order that requires a specified person (including the owner of a computer system) to provide such information and assistance as is necessary and reasonably practicable to enable access to copying or printing of data. Computer equipment and storage devices can be examined off site. Officers can copy all data on a computer if some of the data contains, or is suspected of containing, evidential material. Search warrants can be used to access data accessible from the search premises (including data not physically stored at the search premises).[1]

The *Crimes Act 1914* (Part VIIB, Part 10.6) makes it a criminal offence to interfere with telecommunications, including computer services, the Internet and computer systems. The Act makes it an offence to interfere with email, tamper with data messages or cause a telecommunications message to be sent to an unauthorised person.[2] It is also an offence to use a carriage service to menace or harass another person,[3] or to tamper with or interfere in any way with a facility operated by a carrier.[4] There are also offences of dishonesty[5] in relation to a carriage service provider.[6]

In addition to specific legislation dealing with cybercrime, many other federal laws may be applied to contexts involving computer-related crime, for example, breach of the Copyright Act,[7] and the Trade Practices Act.[8]

Like the Commonwealth, most Australian states and territories also have passed specific computer crime legislation.[9] For example, New South Wales has passed legislation based on the Model Criminal Code Project.[10]

In most Australian jurisdictions, the criminal provisions governing fraud now cover deception in relation to a person, but also deception of a computer or machine leading to falsification of computer-stored data, credit cards and ATM cards.[11] Similarly, provisions dealing with falsification of documents, which

previously applied only to written documents, now cover electronic documents such as data stored on a computer or ATM card.[12] The criminal laws in most jurisdictions have also been amended to include unlawful access to a computer and hacking. Traditional criminal laws dealing with theft, forgery, trespass and burglary may also be applied to cybercrime contexts.[13]

'Soft', or self-regulations and preventive, strategies in Australia include:

- **Content regulation**: A major strategy to prevent misleading and deceptive content being put online is to regulate online content. Software is already available to screen objectionable content. However, misleading and deceptive advertising could be hard to detect.
- **Certification and endorsement services**: These services provide users with information as to the reliability and acceptability of online material. One of the main problems with endorsement and certification is with proliferation of such services and determination of appropriate standards.
- **Management of fraud control**: Explicit fraud control policies and procedures is a major fraud prevention strategy. Specific policies on computer security need to be developed. Similarly, procedures must exist for reporting computer abuse.
- **Staff**: It is important that trustworthy and reliable staff are employed, particularly at senior level.
- **Computer usage monitoring**: Staff use of Internet needs to be monitored through appropriate logs of usage.
- **Personal identification**: Establishing the identity of the user is crucial in fraud prevention. Most procedures involve use of passwords and these usually need to be changed regularly. Similarly, access needs to be denied after a specified number of tries. Another strategy is to use single-use passwords. In recent years, biometric identifiers, which make use of unique physical characteristics like fingerprints, retinal images, facial or hand geometry are being advocated as an alternative. However, these are expensive to use and issues of privacy and confidentiality of data have yet to be resolved. Public Key Infrastructure is another way of ensuring that both consumer and provider are confident of each other's identity, but it is legally complex and administratively burdensome. For this reason, it may be unsuitable for large numbers of small citizen–government and government–citizen transactions.
- **Information services**: Regulatory surveillance could be used to locate objectionable practices and consumers could be educated about it. Regulatory agencies do provide information to users about questionable practices being used by fraudsters.
- **National fraud desk**: The Australian Federal Police national fraud desk project has widened the concept of the database by including a fraud reference component. With this component, fraud investigators and analysts will be kept up-to-date on emerging trends and new techniques in areas such as credit card fraud, identity fraud, computer crime, insurance and bank fraud, proceeds of crime and telecommunications fraud (Australian Federal Police 2000).

International regulation

Given the reality that e-fraud often occurs across national borders, international regulation and law enforcement is required. International regulation involves two broad types: voluntary regulation (self regulation) in the form of international codes; and criminal laws and cooperative enforcement efforts to deal with more serious offences.

Voluntary regulation has come in the form of various industry standards governing such areas as security and guidelines for best business practice, developed by such groups as the International Chamber of

Commerce (1998) and the Direct Marketers Association. Still other guidelines have been developed through organisations such as the OECD.

Building upon its guidelines for e-business, issued in 2000, the OECD in June 2003 approved new guidelines that will provide consumers greater protection from fraudulent and deceptive practices that cross national borders. The new OECD Guidelines seek both to enhance consumer protection within individual countries and to enhance cooperation on detection, prosecution and enforcement efforts between countries (OECD June 2003).

Recommended adequate domestic frameworks for combating cross-border fraudulent and deceptive commercial practices include:

- effective measures to deter businesses and individuals from engaging in fraudulent and deceptive practices
- effective mechanisms to investigate, preserve, obtain and share relevant evidence of such activity
- effective mechanisms to stop those engaged in such activity
- effective mechanisms that provide adequate redress for victims of such fraudulent and deceptive commercial conduct
- identification of obstacles to cross-border cooperation in the area of consumer protection
- provision of education to consumers about fraudulent and deceptive practices
- consideration of how domestic enforcement agencies might use evidence, judgments, and enforceable orders obtained by consumer protection agencies in another country to improve their ability to halt expeditiously the same conduct in their own country.

The Guidelines provide principles for international cooperation in consumer protection; and tackle cooperation for adequate enforcement and consumer redress. The Guidelines call on member countries to give special attention to:

- possible roles played by enforcement agencies providing information and advice to consumers
- effectiveness of existing cross-border consumer redress mechanisms
- feasibility of authorising agencies to gather and share information about assets of the defrauder to aid a foreign consumer protection enforcement agency
- effecting timely freezes on business-related assets located in another country
- improving international arrangements for the enforcement of judgments
- developing additional safeguards against the abuse of payment systems and redress for consumer victims of such abuse.

Criminal sanctions: While there is no uniform treaty addressing e-fraud, the most significant international criminal law development has been the Convention on Cybercrime. The Council of Europe approved the Convention on Cybercrime on 19 September 2001, the treaty being approved by the 43 member states. The treaty creates procedural structures for police officials to pursue computer crime across national borders.[14]

Chapter II, Section I, Title I of the Cybercrime Convention proposes that each country classify as crimes, offences against the confidentiality, integrity and availability of computer data and systems. The treaty calls for international cooperation to detect and punish computer hacking, data theft and the interference with computer systems through fraud or forgery.

Chapter II, Section I, Title II of the Cybercrime Convention proposes a number of computer-related offences for computer related forgery (article 7) and computer-related fraud (article 8). The treaty requires signatory states to regularise criminal law so it would prohibit unauthorised access to computer systems, unauthorised interception of computer transmissions, hacking computer systems or data, making devices facilitating such activity and forging computer data.

While few question the need for greater international cooperation, countries such as the United States have criticised the Convention on Cybercrime as too reliant upon criminal as opposed to market-based enforcement mechanisms.

Options to combat e-fraud in Australia

The following additional measures could prove useful in the fight against e-frauds.

Prevent internal fraud by better management of security. The level of security protection will involve a risk management analysis that balances the level of risk against the cost of prevention. Depending upon the context involved, some of the risk management measures to combat e-fraud include:

- installing and maintaining a network firewall to protect data accessible through the Internet
- keeping security patches up-to-date
- encrypting data sent across public networks
- using and updating anti-virus software
- not using vendor-supplied defaults for passwords and other security parameters
- testing security systems and processes regularly
- maintaining a policy that addresses information security for employees and contracts
- restricting physical access to cardholder information
- managing risk through conducting e-risk assessment, establishing baseline network controls, developing a response plan and getting insurance.

Anti-identity theft legislation: There are divergent views about whether Australia or its states and territories should enact specific identity fraud legislation. Similar legislation was enacted in the United States in 1998. The South Australian Parliament passed legislation in December 2003 to create four new offences specifically targeting those who use, or intend to use, a false identity to commit a serious crime (Office of Consumer and Business Affairs, South Australia 2004).

Driving licence as proof of identity: Although a driving licence is routinely used as proof of identity, it is only a proof of driving ability, and not of identity. The supporting documents used by transport departments in the various states and territories of Australia to establish identity, for the purpose of issuing Driver's Licences, may themselves have been obtained fraudulently. The holograms that distinguish cards such as a drivers licence are not hard to copy and produce in vast numbers. Biometrics, such as thumb impressions (fingerprints), could be used along with photographs on drivers licences. However, as discussed earlier, the use of biometrics raises significant privacy and integrity issues that have yet to be resolved.

National Vigilance Commission: The OECD has appointed a special Financial Action Task Force to deal with, among other things, the issue of customer identification. 'Know Your Customer' guidelines are the cornerstone of the Financial Action Task Force recommendations (OECD 2003). A similar task force or commission, at the national level in Australia, could help focus on this very important problem of identity

fraud. The Australian Federal Police has a central high-tech crime centre but it has a wide mandate, which ranges from child pornography to card fraud.

Identity requirement for Internet account: A step in the right direction is the proposal put before the Parliamentary Commission on Cybercrime in July 2003 requiring anyone wanting to open an Internet account in Australia to produce 100 points of identification (Electronic Frontiers Australia 2003).

Identity requirement for content providers: Under France's Liberty of Communication Act, web content providers must provide identification to Internet service providers who will host their material. Similar provisions could help Australia (Electronic Frontiers Australia 2003).

Information systems for fraud: It is important that departments have clear and transparent fraud control policies in place. Regular reporting systems about incidence of fraud exist in banks. For example, the Core Principles for Effective Banking Supervision laid down by the Australian Prudential Regulation Authority (2001) state that procedures need to exist, inter alia, for '... prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities'.

Award for whistle blowers: Although protection for whistle-blowers has been introduced through appropriate statutes, the provisions need to be given wide publicity. Just as copyright notices are displayed at various locations in organisations, so should whistle blowers' rights be displayed. For example, the Australian Prudential Regulation Authority has provided (on their web site) information about various means by which public informants could help.

Precautions in opening bank accounts: The 100 point system being used to open bank accounts may not be adequate to stop identity fraud. At the time of opening an account, it may be useful to require an introduction from existing account holders. This will enable tracing of fictitious account holders if a fraud subsequently comes to light.

Awareness-raising campaigns: Just as issues of a critical nature are widely advertised (for example, AIDS, quarantine, etc.), identity fraud could be prominently brought to peoples attention to make them aware of the problem. As Graycar (2002, p. 9) suggests 'people need to be taught how to protect themselves and how to avoid situations of high risk'.

Conclusion

As governments increasingly deliver services electronically, they will face new levels and types of risks. Coping with these risks will require a convergence of good policy and effective governance that includes commonsense operational management characterised by best practice in risk management, constant adjustment between such issues as privacy and business efficacy, ongoing staff development, and increasing international cooperation.

Acknowledgments

The authors gratefully acknowledge the contribution, by Michael Krstic, of some valuable information towards preparation of this paper.

References

Attorney-General's Department 2000, *The changing nature of fraud in Australia*, Commonwealth of Australia, Canberra, <http://www.law.gov.au/agd/Department/Publications/publications/Fraud.htm>, accessed on 23 February 2004.

Attorney-General's Department 2002, *Commonwealth Fraud Control Guidelines 2002*, Commonwealth of Australia, Canberra.

Auditor General for Western Australia 2003, *Contracting not-for-profit Organisations for Delivery of Health Services*, Report No. 2, April 2003, <http://www.audit.wa.gov.au/reports/report2003_02.html>, accessed on 6 April 2004.

Australian Federal Police 2000, 'National Fraud Desk: the collective approach towards fighting fraud', *Comfraud Bulletin*, 16, <http://www.afp.gov.au/raw/publications/comfraud/comjan00.htm>, accessed on 23 February 2004.

Australian Institute of Criminology 2003, Counting the cost of crime in Australia, AIC, Canberra, <http://www.aic.gov.au/media/2003/20030409.html>, accessed on 23 February 2004.

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

Australian National Audit Office 2003, Survey of Fraud Control Arrangements in APS Agencies, ANAO, Canberra, <http://www.anao.gov.au/WebSite.nsf/Publications/A99ABD97799669E2CA256DE900754906>, accessed on 22 February 2004.

Australian Prudential Regulation Authority 2001, *Core Principles for Effective Banking Supervision*, APRA, Canberra.

Australian Taxation Office 2002, 'Queensland man jailed for GST fraud', <http://www.taxpack.com.au/index.cfm/pageId/whatsnew-whats_new_jul02>, accessed on 22 February 2004.

Clarke, R 1987, 'Just another piece of plastic for your wallet: the Australia card scheme', *Prometheus*, vol. 5, no. 1, June, <http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html>, accessed on 5 April 2004.

Dixon, N 2001, *Employees and the Internet: Issues for Public and Private Sector Employers*, Queensland Parliamentary Library, <http://www.parliament.qld.gov.au/Parlib/Publications_pdfs/books/rbr1201nd.pdf>, accessed on 23 February 2004.

Ellison, J 2003, 'Customs: Theft of servers', Minister for Justice and Customs, Media Release, <http://www.ag.gov.au/www/justiceministerHome.nsf/Alldocs/RWPACA43E44B87D13E0CA256E0A00030A21?OpenDocument>, accessed on 23 February 2004.

Electronic Frontiers Australia 2003, Submission to the public consultation draft Cybercrime Code of Practice, <http://www.efa.org.au/Publish/efasubm-iiaccc.html>, accessed on 5 April 2004.

Grabosky, P, Smith RG & Dempsey G 2001, *Electronic theft: unlawful acquisition in cyberspace*, Cambridge University Press, Cambridge.

Graycar, A 2002, *Identity related Fraud: risks and remedies*, Australian Institute of Criminology, Canberra.

KPMG 1999, Fraud Survey, <http://www.aic.gov.au/research/fraud/kpmg_aus_1999.pdf>, accessed on 23 February 2004.

Hawker Committee 2001, Certainty of Identity: A Fundamental of Security, <http://www.austlii.edu.au/au/other/CyberLRes/2001/22>, accessed on 14 December 2003.

House of Representatives Standing Committee on Economics, Finance and Public Administraion 2000, *Review of ANAO Audit Report No.37 1998–99 on the management of Tax File Numbers*, Parliament of Australia, <http://www.aph.gov.au/house/committee/efpa/tfnaudit/recs.htm>, accessed on 23 February 2004.

International Chamber of Commerce 1998, *Guidelines on Advertising and Marketing on the Internet*, <http://www.iccwbo.org/home/menu_advert_marketing.asp>.

McGinty, J 2003, *Funding for the Western Australian Aboriginal Community Controlled Health Organisation*, Government of Western Australia, <http://www.ministers.wa.gov.au/Speeches/A06/waccho.pdf>, accessed on 23 February 2004.

Minister for Justice and Customs 2003, *Government and industry tackle fraud against financial institutions*, <http://www.ag.gov.au/www/justiceministerHome.nsf/0/7D56D3B406D4B96BCA256D26002324B0?OpenDocument>, accessed on 22 February 2004.

Office of Consumer and Business Affairs, South Australia 2004, <http://www.ocba.sa.gov.au/consumeradvice/identitytheft/legislation.html> accessed on 23 February 2004.

Organisation for Economic Cooperation and Development June 2003, *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Geneva, <http://www.oecd.org/dataoecd/24/33/2956464.pdf>.

Organisation for Economic Cooperation and Development 2003, Evaluation of measures taken by FATF members dealing with customer identification, OECD, Geneva, <http://www.networkusa.org/fingerprint/page1b/fp-fatf-identification.htm>, accessed on 13 December 2003.

Smith, R 2000, *Electronic fraud*, paper presented at Australian Society of Certified Public Accountants, CPA Congress 2000, Sydney.

Smith, R 1999, *Defrauding Governments in the Twenty-First Century*, paper presented at 14th Annual Conference of the Australian and New Zealand Society of Criminology, Perth.

Standing Committee on Economics, Finance and Public Administration 2000, Official Committee Hansard: Tax File Number Inquiry, Commonwealth of Australia, <http://www.aph.gov.au/hansard/reps/commttee/r665.pdf>, accessed on 22 February 2004.

Notes

[1] See also Joint Committee on National Crime Authority, investigation on law enforcement implications of new technology, <www.aph.gov.au/senate/committee/nca.ctte/>; Electronic Frontiers Australia comment on the Cybercrimes legislation <www.efa.org.au/Analysis/cybercrime/bill.htm>.

[2] Criminal Code 1995 (Cwth) s.85ZD.

[3] Criminal Code 1995 (Cwth) s.85ZE.

[4] Criminal Code 1995 (Cwth) s.85ZJ.

[5] Dishonesty is defined in terms of ordinary people.

[6] Criminal Code 1995 (Cwth) s.474.

[7] Note that the *Copyright Act 1968* (Cwth) defines 'literary work' as including 'a computer program or compilation of computer programs' (s.10).

[8] See *Trade Practices Act 1974* (Cwth), s.53–65 which create a number of offences relating to consumer protection. See also equivalent legislation in the Fair Trading Acts of most jurisdictions.

[9] See, for example, *Crimes Act 1958* (Vic.) s.197; *Crimes Act 1990* (NSW) s.194,201; Criminal Code (WA), s.441, 443, 455; Criminal Code (Tas) s.267–69.

[10] *Crimes Amendment (Computer Offences) Act 2001* (NSW).

[11] See, for example, *Crimes Act 1958* (Vic.) s.81(4); Criminal Code (Tas.) s.257B.

[12] See, for example, *Crimes Act 1914* (Cwth); *Crimes Act 1958* (Vic.) s.83A; Criminal Code (WA) s.443.

[13] See, for example, Criminal code (WA) s.473 in which 'forgery' is defined in such a way that it would cover alteration of computer records.

[14] <http://conventions.coe.nt/Treaty/EN/rojets/FinalCybercrime.htm>.
Background Information and full text of the convention can be found at Council of Europe's web site <http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime>.