PARLIAMENT OF VICTORIA

DRUGS AND CRIME PREVENTION COMMITTEE

INQUIRY INTO FRAUD AND ELECTRONIC COMMERCE

Final Report

January 2004

by Authority
Government Printer for the State of Victoria

No. 55 Session 2003-2004

The Report was prepared by the Drugs and Crime Prevention Committee.

Drugs and Crime Prevention Committee
Inquiry into Fraud and Electronic Commerce: – Final Report
DCPC, Parliament of Victoria

ISBN: 0-646-43091-2

Drugs and Crime Prevention Committee
Level 8
35 Spring Street
Melbourne Victoria 3000
Telephone: (03) 9651 3541
Facsimile: (03) 9651 3603
Email: sandy.cook@parliament.vic.gov.au
http://www.parliament.vic.gov.au/dcpc

Drugs and Crime Prevention Committee – 55th Parliament

Ms Carolyn Hirsh, M.L.C.– **Chair**

The Hon. Robin Cooper, M.L.A. – **Deputy Chairman**

Ms Kirstie Marshall, M.L.A.

Mr Ian Maxfield, M.L.A.

The Hon. Sang Minh Nguyen, M.L.C.

Dr Bill Sykes, M.L.A.

Mr Kim Wells, M.L.A.

Drugs and Crime Prevention Committee – 54th Parliament

The Hon. Cameron Boardman, M.L.C. – **Chairman**

Mr Bruce Mildenhall, M.L.A. – **Deputy Chairman**

The Hon. Robin Cooper, M.L.A.

Mr Kenneth Jasper, M.L.A.

Mr Hurtle Lupton, M.L.A.

The Hon. Sang Minh Nguyen, M.L.C.

Mr Richard Wynne, M.L.A.

Committee Staff

Ms Sandy Cook
Executive Officer

Mr Pete Johnston
Senior Legal Officer (Inquiry into Amphetamine and 'Party' Drug Use)

Ms Michelle Heane
Office Manager

Consultants, Inquiry into Fraud and Electronic Commerce

Dr Russell G. Smith (Discussion Paper and Final Report)
Deputy Director of Research
Australian Institute of Criminology

Mr Jamie Walvisch (Final Report)
Research Analyst
Australian Institute of Criminology

Mr Stuart Candy (Discussion Paper)
Research Assistant
Australian Institute of Criminology

Functions of the Drugs and Crime Prevention Committee

The Victorian Drugs and Crime Prevention Committee is constituted under the *Parliamentary Committees Act 2003* (Vic)

Section 7.

The functions of the Drugs and Crime Prevention Committee are, if so required or permitted under this Act, to inquire into, consider and report to the Parliament on any proposal, matter or thing concerned with –

(a) the use of drugs, including the manufacture, supply or distribution of drugs;

(b) the level or causes of crime or violent behaviour.

Terms of Reference

Received from the Legislative Assembly on Wednesday 17 April 2003.

To the Drugs and Crime Prevention Committee – for inquiry, consideration and report by 31 December 2003 on:

(a) the extent and nature of fraud and white-collar crime in Victoria;

(b) the impact of new technology supporting E-commerce on the opportunities for fraud;

(c) the current and proposed state, Commonwealth and international strategies and initiatives in relation to dealing with fraud and white-collar crime; and

(d) the need for policy and legislative reform to combat fraud and white-collar crime in Victoria.

Chair's Foreword

The Inquiry into Fraud and Electronic Commerce was commenced in 2002 by the Drugs and Crime Prevention Committee of the 54th Parliament. A great deal of work was undertaken and a Discussion Paper was produced, providing a comprehensive literature review, clarification and expansion of the Terms of Reference, and a great deal of preliminary evidence.

Following the 2002 election, a new Drugs and Crime Prevention Committee, established by the 55th Parliament, was asked to continue the work already commenced. The same Terms of Reference were resubmitted to the Committee to enable work to be completed. This Report is the result.

Fraud, and the somewhat broader concept, 'white-collar crime', have profound effects on the community, both in terms of financial loss to large organisations and government and its life-changing effects (in many cases) on individual victims. It is estimated that fraud cost the Victorian community as much as $641 million last year, although there are no truly accurate data. Because fraud is not limited to any Australian state, or indeed Australia's national boundaries, the Committee believes that the major responses to fraud should be co-ordinated nationally. The Committee's recommendations are therefore formulated to reflect national and international best practice.

Despite the proliferation of fraud in the corporate sector, the investigation of corporate crime would be far broader than would be possible in this Inquiry. The Committee believes that corporate crime is best dealt with by such organisations as the Australian Securities and Investments Commission, the Australian Crime Commission, and other national organisations specifically established to deal with corporate crime. This Report focuses on fraud committed by individuals, with particular attention given to identity-related fraud and credit card fraud that relate to electronic commerce.

The Report focuses particularly on financial crimes committed using electronic technologies. The dramatic and continually increasing use of electronic commerce by individuals, small businesses, large corporations and government, invariably requiring electronic funds transfer, has led to an increase in all three factors which enable fraud to take place – motivated offenders, suitable targets and the absence of adequate constraints or guardians.

Evidence to the Committee demonstrated that it is impossible to develop a truly effective response to fraud until a more accurate picture of its nature and extent is available. Many of the Committee's recommendations concern the collection, analysis and dissemination of data related to all types of fraud in Victoria. A major recommendation concerns the establishment of a Victorian Fraud Information and Reporting Centre within the Victorian Police. The Committee envisages that this centre would be staffed primarily by civilians with an understanding of criminology and expertise in areas such as law, commerce, banking and statistics.

The Committee believes that one of the greatest deterrents to fraud within organisations is a commitment by upper-level management to the prevention of fraud, an understanding of how to achieve the goal of fraud prevention, a set of policies to this end, and communication with employees both directly and through modeling of a fraud prevention ethic.

An important fraud control measure lies in education of members of the community to decrease their vulnerability to becoming victims of fraud. The more awareness in the community about the types of fraud likely to be perpetrated, the less likely is a potential perpetrator to succeed in a 'scam'. Many people do not report fraud, as they feel it is somehow their own fault and they do not want others to see them as 'foolish'. The Committee has recommended that the central collection and analysis agency also take responsibility for dissemination of information about fraud to the public.

The Committee hopes that this Report will provide a basis for Victorians to prevent becoming victims of fraud, to be discouraged from attempting to commit fraud, and to establish adequate security measures to make the commission of fraud impossible.

I want to express my sincere thanks to Dr. Russell Smith and Mr Jamie Walvisch, consultants for this Inquiry, for their commitment to the project and for drafting this Report, and to Committee staff – Ms Sandy Cook, Executive Officer, for her outstanding efforts and attention to detail in all aspects of the preparation of this Report, and Ms Michelle Summerhill, Ms. Rhonda MacMahon and Ms Sandy Jensen, Office Managers, for their assistance with the Inquiry.

I would also like to thank the members of both Committees for their participation and contribution to the Inquiry. In particular the previous Chair, for his committed stewardship of the preliminary research and the production of Discussion Paper which formed the basis of this Report.

I hope that all key individuals and organisations concerned about fraud and 'white-collar crime' closely consider the contents of this Report, as the Committee believes significant community benefit will flow from the implementation of the recommendations made.

Carolyn Hirsh M.L.C.
Chair

Executive Summary and Recommendations

Fraud and white-collar crime have far-reaching effects on the community, not only in terms of the financial impact on business and government, but also because of the effects on individuals who are victimised. It is estimated that these crimes cost Victoria as much as $641 million last year – money which could be better used for essential community works in promoting health, education and security. It is the purpose of this Inquiry to examine the trends in this area, and to look at how Victorian law and policy can best respond.

Due to the ease with which fraud transcends domestic and international jurisdictional boundaries, especially in the context of electronic commerce, the Committee believes that the best response should be a national, integrated approach that uses the resources of the many federal, state and territory bodies working in this area in a co-ordinated fashion. No one agency, acting alone, can expect to be able to tackle crimes of dishonesty effectively. The Committee is therefore concerned to ensure that any Victorian response reflects best practice and is in accord with measures implemented in other places in response to these global concerns. The Committee is also concerned to ensure that any safeguards or controls that are put in place to minimise fraud risk, should not be so onerous as to preclude or frustrate any legitimate activities of business and government.

In this Report the Committee has considered many aspects of fraud prevention and control. These aspects have included an examination of the nature and extent of fraud, the use of fraud prevention policies and technologies, the detection and reporting of fraud, the investigation of suspected fraudulent conduct and the legislative and judicial responses to fraud. Each of these areas, and others, are outlined briefly below, followed by relevant recommendations proposed by the Committee.

The nature and extent of fraud

Although not specifically defined by legislation in Victoria, fraud is a generic category of conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage over another person or entity. The

Committee heard that fraudulent conduct can be committed in a wide range of circumstances. Fraud can be committed by individuals or by corporations, and it can occur in the public sector, the professional sector or the corporate and business sector. It can range from small-scale misappropriation of goods and services to multi-million dollar cases of embezzlement. In an attempt to limit the scope of the Inquiry, this Report focuses on financial crimes perpetrated by individuals, rather than by corporations.

Examples of the types of fraud examined in the Report include procurement fraud, insurance fraud, cheque fraud, funds transfer fraud, loan and investment fraud, refund fraud, false invoicing, telemarketing fraud and art fraud. Identity-related fraud and credit card fraud were identified to the Committee as being of particular concern.

Specific attention is paid in the Report to financial crimes involving the technologies of electronic commerce. These technologies bring with them new risks, due to the lack of physical presence of people in transactions and the ability of people to disguise or manipulate their identity when conducting business online. Fraud can occur by individuals transmitting misleading and deceptive information online, by failing to honour contractual agreements entered into electronically, or through the misappropriation of funds transmitted electronically.

The motivations for committing fraud are varied. They include greed, financial strain in one's personal or business life and maintaining a lifestyle beyond one's means. The Committee was told of an increase in recent years of organised criminals in fraudulent activity involving external attacks on banks, superannuation funds and businesses. The Committee was also informed of an increase in fraud motivated by problem gambling.

Many of those who gave evidence to the Committee stated that fraud is increasing in Victoria. There are, however, many impediments to the accurate measurement of fraud. Particular difficulties are created by the fact that fraud tends to be a category of crime that often goes undetected. Even when it is detected, it will often not be reported to law enforcement agencies. This may be due to a belief that the matter is not serious enough to warrant police attention, fears of a consumer backlash, bad publicity, inadequate proof, or a reluctance to devote time and resources to prosecuting the matter.

Another part of the problem lies in the absence of agreed definitions, which has prevented data from being collected in a uniform and consistent way. In Victoria, police statistics record 137 separate offences included in the category 'deception' and 170 other offences that have some relevance to fraud and dishonesty.

These limitations prevent the extent of fraud in Victoria being ascertained with precision. It is, however, possible to make an estimation using the information that is available from police statistics and fraud victimisation surveys, and taking into account the low rate of reporting. Based on such calculations, it is

estimated in the Report that the total fraud costs for Victoria could have been as high as $641 million last year.

Fraud information and reporting centres

The Committee believes that before the problem of fraud can be addressed effectively much more extensive information needs to be gathered on the nature and extent of the problem and how it is handled. Accordingly, a number of recommendations have been made in relation to the collection and publication of statistics (for a full list of the Recommendations in numerical order see Appendix H).

Of particular importance is the Committee's recommendation that a Victorian Fraud Information and Reporting Centre (VFIRC) be established within Victoria Police to co-ordinate and respond to all aspects of fraud reporting, prevention and the provision of information and statistics. VFIRC would be staffed by civilian analysts with backgrounds in law, commerce, banking, statistics and criminology, rather than sworn police officers. VFIRC would not have a policing and intelligence function, but rather would be the central agency in Victoria for the collection and dissemination of information on fraud and financial crime and aspects of fraud prevention. It would also be the central agency in Victoria to which all reports involving suspected fraud from members of the public, as well as from public and private sector agencies, should go. VFIRC analysts would receive reports, compile statistical information, and then transmit reports to relevant agencies for investigation, be they police, professional boards, or federal investigatory agencies.

It is hoped that the creation of VFIRC would assist not only in the compilation of accurate information and statistics on fraud in Victoria, but would also improve fraud reporting and reduce the incidence of crimes of this nature through the wide-scale dissemination of fraud prevention information and advice. By having a more precise understanding of the scale of the problem of fraud in Victoria, fraud prevention resources could be allocated more effectively and new initiatives developed to control new methodologies of financial crime as they occur and, hopefully, to prevent them from being initiated. The Committee believes that the money saved through these initiatives could amount to a considerable proportion of the estimated $641 million being lost each year in Victoria at present.

The Committee has also recommended the establishment of a similar Centre at a national level (an Australian Fraud Centre), to help co-ordinate a national response to fraud. Such a Centre could provide a central information and intelligence repository for all forms of fraud and financial crime. It could also facilitate the exchange of national trend information relating to financial crime, to help in its prevention.

Recommendations

The Committee recommends the establishment of a Victorian Fraud Information and Reporting Centre (VFIRC), within Victoria Police, as a dedicated agency staffed by unsworn analysts, to:

i collect and disseminate information about the nature and extent of fraud occurring across Victoria;

ii collect and publish statistics on fraud; and

iii receive complaints of fraud from members of the public and public and private sector organisations for referral to appropriate agencies for investigation (Recommendation 3a, p.88).

The Committee recommends that VFIRC would not have an operational policing function in the investigation of cases of fraud. It should not be located within the Major Fraud Investigation Division of Victoria Police (Recommendation 3b, p.88).

The Committee recommends that VFIRC should be responsible for the collection and publication of statistics in relation to the nature and extent of fraud in Victoria, including information on prosecution and sentencing of fraud offenders (Recommendation 3c, p.88).

The Committee recommends that VFIRC should play a central role in relation to the reporting of fraud. All reports of fraud and financial crime in Victoria should be received by VFIRC either by direct notification from members of the public or as notified by other agencies (Recommendation 3d, p.88).

The Committee recommends that VFIRC should be located centrally in dedicated premises in order to facilitate access and to enhance visibility (Recommendation 3e, p.88).

The Committee recommends that VFIRC should receive a dedicated budget administered by Victoria Police (Recommendation 3f, p.88).

The Committee recommends that VFIRC should be the central Victorian agency responsible for the collection and analysis of reports of fraud perpetrated against public sector agencies in Victoria and by Victorian public servants. Individual government agencies in Victoria should be required to notify VFIRC of all cases involving suspected fraud that are required to be reported to the Minister for Finance. VFIRC analysts would then compile reports for the Minister for Finance as required under the *Financial Management Act 1994* (Vic.) (Recommendation 3g, p.88).

The Committee recommends the establishment of an Australian Fraud Centre (AFC), to collect and disseminate information about the nature and extent of fraud occurring across Australia and to help co-ordinate a national response to fraud. In order to facilitate the establishment of the AFC, the Attorney-General for the State of Victoria should propose its establishment at the next meeting of the Standing Committee of Attorneys-General (Recommendation 4a, p.90).

The Committee recommends that the AFC should be involved in the collection and dissemination of fraud intelligence and the publication of national fraud statistics (Recommendation 4b, p.90).

The Committee recommends that the AFC should be housed within the infrastructure of either the Australian Crime Commission or the Australian Federal Police (Recommendation 4c, p.90).

The Committee recommends that the Attorney-General for the State of Victoria seek a review of the Australian Standard Offence Classification, to enable more specific information on fraud and electronic commerce-related offences to be identified (Recommendation 1a, p.61).

The Committee recommends that the Attorney-General for the State of Victoria also request the Australian Bureau of Statistics to include fraud and other deception offences in its regular surveys of household and personal victimisation (Recommendation 1b, p.61).

The Committee recommends that any changes made to the Australian Standard Offence Classification be reflected in statistics that are collected and published by police, courts and correctional agencies in Victoria (Recommendation 1c, p.61).

The Committee recommends that legislation governing professional regulatory bodies, such as the Medical Practitioners Board of Victoria and the Legal Practice Board, be amended to require the annual publication of specific information about fraud and dishonesty-related complaints that have been referred for investigation, how those complaints were dealt with and the outcomes of investigations (Recommendation 2a, p.64).

Fraud prevention policies and codes of conduct

Although legally-based deterrence should always have a place in controlling economic and white-collar crime, it is clearly preferable to try to prevent such crimes from being committed in the first place. Accordingly, the Committee believes that organisations should be encouraged to adopt a range of preventive measures, leaving formal policing and prosecution for the hopefully rare instances in which organisational regulatory controls fail.

The Committee believes that responsibility for the prevention of much white-collar crime, and particularly economic crime, lies in the first instance with upper-level management within organisations. If chief executive officers and managers at all levels have a commitment to the prevention of economic crime, and understand how that goal may be achieved, this will provide a foundation and model for their employees to follow. While it is not possible to force people to have such a commitment to fraud prevention, it is possible to put in place policies and procedures that can encourage compliance with such an ethic, and help to minimise fraud taking place.

The Committee heard evidence about the use of fraud prevention policies in Victoria and around Australia. While public sector policies are mandatory in some jurisdictions, in Victoria there is no such requirement. Fraud prevention is simply one aspect of the general financial management framework. While the Committee acknowledges that, if properly implemented, the current framework may well adequately address the risks of public sector fraud, it believes that these risks would be better addressed if all public sector entities were required to develop specific fraud control policies. Such a requirement would ensure that all public sector entities specifically address the possibility of fraud, and the steps they will take to prevent and control it, which may not occur under the current scheme. The Committee believes that such policies should also be implemented as widely as possible in the private sector.

Codes of practice can also be used to set acceptable rules and procedures for preventing and responding to fraud. Not only are they able to provide a widely disseminated statement of existing laws and acceptable practices, which helps to create a culture of compliance within specific industries, but they also often include dispute resolution procedures and sanctions for non-compliance with the rules in question. The Committee has made a number of recommendations about the development and use of specific industry codes in Victoria.

Recommendations

The Committee recommends that a requirement that all public sector entities (including local government) implement and maintain a fraud control policy be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standard AS8001-2003 *Fraud and Corruption Control* and the New South Wales Audit Office's *Fraud Control: Developing an Effective Strategy,* and should include elements relating to the prevention, detection, reporting and investigation of fraud, as well as containing a fraud response plan. It should also specifically address the risks of fraud arising out of the use of electronic commerce (Recommendation 6a, p.139).

The Committee recommends that all public sector entities be required to certify their compliance with the relevant fraud control direction in the annual certification process established by the Financial Management Compliance Framework (Recommendation 6b, p.140).

The Committee recommends that VFIRC promote the implementation of fraud control policies by businesses and corporations in the private sector, using Standard AS8001-2003 *Fraud and Corruption Control* as a model. VFIRC should provide assistance to such organisations in drafting and implementing such policies if necessary (Recommendation 7a, p.141).

The Committee encourages the development of a fraud control certification service for the private sector, to certify compliance with Standard AS8001-2003 *Fraud and Corruption Control*. If such a service is established, its existence should

be promoted by VFIRC and certification encouraged. A list of those organisations that have had their policy certified should be published on VFIRC's web site (Recommendation 7b, p.141).

The Committee recommends that appropriate sanctions be introduced for failure to comply with the Code of Conduct for the Victorian Public Sector (Recommendation 8, p.144).

The Committee recommends that an Internet industry body be established in Victoria. Steps should be taken to facilitate the establishment of such a body, including the provision of seed funding if necessary. Any body that is established should be encouraged to develop a Victorian Internet Industry Code of Conduct which deals with fraudulent content and unsolicited material transmitted electronically (Recommendation 9a, p.148).

The Committee recommends the promotion and use across Victoria of the Department of Treasury's *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business*, as well as the Internet Industry Association's *Cybercrime Code* when finalised (Recommendation 9b, p.148).

The Committee recommends that industry Codes of Conduct relating to electronic commerce, the Internet and online gambling be mandated under Part IVB of the *Trade Practices Act 1974* (Cth) (Recommendation 10, p.150).

Information security management

The Committee was advised that fraud often occurs as a result of individuals obtaining confidential information. For example, credit card fraud will generally arise where a person has obtained someone else's credit card details without their authorisation. Identity-related fraud can involve the use of an individual's personal information, such as their birth date or mother's maiden name. Certain types of corporate fraud can occur where a company officer gains unauthorised access to sensitive information. One of the simplest and most effective ways in which these types of fraud can be prevented is by protecting the information that is used to perpetrate the fraud. If individuals have no way of obtaining the information necessary to commit the crime they will be thwarted in their attempts.

The Report outlines a number of steps that can be taken to protect such information. Where information is held by an organisation, it was suggested to the Committee that an information security management strategy could be put in place. Such a strategy would set out procedures for protecting all types of information, ranging from letters received by an organisation to the organisation's computerised accounting system. The Committee has recommended that all public sector entities be required to implement an information security management strategy, and that private sector organisations also be encouraged to develop such a strategy.

Recommendations

The Committee recommends that all public sector entities (including local government) be required to implement and maintain an information security management policy and that this requirement be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standards AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management;* AS/NZS 7799.2:2003 *Information security management – Part 2: Specification for information security management systems*; and HB 231:2000 *Information security risk management guidelines* (Recommendation 11a, p.156).

The Committee recommends that all public sector entities (including local government) be required to certify their compliance with the relevant Information Security Management Direction in the annual certification process established by the Financial Management Compliance Framework (Recommendation 11b, p.156).

The Committee recommends that VFIRC promote the implementation of information security management strategies by businesses and corporations in the private sector, using the Standards Australia Information Security Management Standards as a model (Recommendation 12a, p.156).

The Committee recommends that VFIRC should also encourage businesses and corporations in the private sector to have their information security management systems certified as being in compliance with the Standards Australia Information Security Management Standards. A list of those organisations that have had their systems certified should be published on VFIRC's web site (Recommendation 12b, p.156).

The Committee recommends that all financial institutions operating in Australia encrypt all data moving to and from EFTPOS and ATM terminals (Recommendation 13, p.156).

Identity authentication

The Committee was made aware that identity-related fraud is one of the key problems, both in Australia and internationally. Such fraud takes place when an offender defeats the user authentication strategies of a system, whatever they may be, and successfully identifies himself or herself as someone else, whether in the guise of a real other person or under cover of a totally fabricated identity. Where user authentication procedures (such as password controls) are circumvented, the offender can avoid responsibility for his or her actions. One way in which to address this problem is to improve the methods by which people are identified, or authenticate their identity, so that people who attempt to use false identities are likely to be detected.

At present there are three usual means of identification: knowledge-based, token-based and biometric. Knowledge-based systems rely on individuals knowing a specific piece of information. Such systems commonly require users

to provide a password or a PIN. Token-based systems rely on individuals having a particular token or document, such as a security pass or driver's licence. Biometric systems measure unique physiological or behavioural characteristics, such as fingerprints or iris patterns.

The Committee has recommended that organisations be encouraged to carry out a risk assessment procedure, to help determine which type of authentication system would be most appropriate to their needs. The Committee has also made a number of recommendations about specific user authentication systems. For example, the Committee has recommended that organisations which rely on knowledge-based systems should implement password management strategies. In relation to token-based systems, the Committee has recommended a number of steps designed to minimise the risks of theft or alteration of documents commonly used as evidence of identity, including the use of document security features. The Committee has not recommended the introduction of personal identity cards.

The Committee has also recommended that biometric systems not be widely used until the technology is more accurate and reliable, appropriate standards have been developed, and biometric-specific privacy protections have been incorporated into legislation.

The Committee was also made aware of a number of other technologies which could be used to help prevent fraud, including computer-chip plastic cards ('smart cards'), public key systems ('PKI') and web seals. Recommendations have been made in each of these areas. The Committee has also recommended that organisations institute pre-employment screening procedures, to assist in the detection of individuals who might be at risk of behaving dishonestly.

Recommendations

The Committee recommends that individual identification cards should not be introduced at a national or state level in Australia (Recommendation 14, p.164).

The Committee recommends that a national approach be taken to the verification of documents used to establish identity, and encourages the Victorian government to co-operate fully with Australian government initiatives designed to enable the online verification of evidence of identity information and to improve the '100-point system' established under the *Financial Transaction Reports Regulations 1990* (Cth) (Recommendation 15a, p.166).

The Committee recommends that public sector agencies and private sector organisations which issue documents that can be used as evidence of identity (such as birth certificates and driver's licenses) take steps to cleanse their databases of information to ensure that information is accurate and current, and that they co-operate with the development of online verification systems (Recommendation 15b, p.166).

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to ensure that effective security measures are used in those documents to minimise the risk of documents being altered or counterfeited (Recommendation 16a, p.169).

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to comply with high level standards with respect to the security of materials used for the creation of such documents (including blank paper, inks, and plastic cards and their components), and that issuing branch offices be required to adopt uniform security standards (Recommendation 16b, p.169).

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity take steps to minimise the extent to which documents are sent to clients by ordinary mail, and that alternative procedures be developed to minimise loss and misappropriation of documents in transit (Recommendation 16c, p.169).

The Committee recommends that biometric systems not be widely implemented by the Victorian Public Service for fraud control purposes until the technology is more accurate and reliable, appropriate standards have been developed, and biometric-specific privacy protections have been incorporated into legislation (Recommendation 17, p.177).

The Committee recommends that the Victorian government should support the early roll-out of EMV standard computer-chip plastic cards for use in electronic transactions in conjunction with Personal Identification Number (PIN) authentication (Recommendation 18, p.179).

The Committee recommends the adoption of the proposals set out in the *Gatekeeper Strategy* concerning secure electronic transactions, and supports the adoption of the *Gatekeeper*-compliant framework at a state level (Recommendation 19a, p.182).

The Committee recommends that Registration Authorities which issue public-private key pairs for use in secure electronic transactions be required to adopt the same standards for identification of users as are required to open an account with a financial institution under the Financial Transaction Reports Regulations 1990 (Cth) (Recommendation 19b, p.182).

The Committee recommends that legislation be passed making it illegal to generate and retain a copy of a private key without consent, once the original has been passed on (Recommendation 19c, p.182).

The Committee recommends that VFIRC establish and maintain a system for the accreditation of web seals that comply with accepted standards concerning content and honesty, and that this system be promoted for use by all Victorian online trading organisations (Recommendation 21a, p.188).

The Committee recommends that consideration be given to creating a criminal offence for an individual or corporation to apply a web seal to an Internet site without appropriate authorisation from the accrediting agency (Recommendation 21b, p.188).

The Committee recommends that VFIRC should promote the use in the public and private sectors of effective measures to screen personnel prior to employment, to assist in the detection of individuals who might be at risk of behaving dishonestly (Recommendation 20, p.185).

Registers

It was suggested to the Committee that the creation and maintenance of registers containing specific information that can be used for fraud prevention would also assist in minimising fraud. Such registers could help in the dissemination of specific information that could be used for fraud detection purposes. The Committee has recommended the establishment of the following registers: an identity fraud register, containing information about fraudulent identities that have been created; a victims of identity fraud register, containing information about people who have had their identities stolen; a stolen/lost document register, containing specific details of evidence of identity documents that have been compromised or lost; a document image register, containing images of evidence of identity documents from around Australia; and banned, deregistered or disqualified people registers, containing information about certain perpetrators of fraudulent or dishonest conduct. Access to the information contained in these registers would depend upon the circumstances and be generally controlled by VFIRC officers in accordance with privacy principles.

Recommendations

The Committee supports the permanent establishment of various registers concerning identity-related fraud, to be administered either by the Australian Crime Commission or the Australian Federal Police. They would include a register of fraudulent identities and associated fraudulent documents, a victims of identity fraud register, a stolen/lost document register and a document image register (Recommendation 24a, p.201).

The Committee recommends that in order to facilitate the establishment of these registers, the Attorney-General for the State of Victoria propose their establishment at the next meeting of the Standing Committee of Attorneys-General (Recommendation 24b, p.201).

The Committee recommends that the Australian Securities and Investments Commission be notified of all people disqualified from managing corporations due to dishonesty-related convictions, for inclusion in the Disqualified Persons Register (Recommendation 25a, p.204).

The Committee recommends a similar registration system be introduced in Victoria within the Office of Consumer and Business Affairs, in which people can be disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations if they have been convicted of an offence that involves dishonesty and is punishable by imprisonment for at least three months (Recommendation 25b, p.204).

The Committee recommends that the Office of Consumer and Business Affairs Victoria be notified of any people who have been disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations due to dishonesty-related convictions, for inclusion in a Victorian Disqualified Persons Register which it develops and maintains (Recommendation 25c, p.204).

The Committee recommends that all Victorian professional regulatory agencies, such as the Legal Practice Board and the Medical Practitioners Board of Victoria, be required to notify VFIRC when one of their members has been deregistered due to fraud or dishonesty-related conduct, for inclusion in a register to be maintained by VFIRC. Each professional association should also be required to maintain its own registers of those who have been deregistered due to fraud or other dishonesty-related offences (Recommendation 25d, p.204).

The Committee recommends that information on VFIRC's register be made available to persons seeking it for legitimate reasons and that the disclosure of information by VFIRC be carried out in accordance with privacy principles (Recommendation 25e, p.204).

Business and Internet domain name registration

The Committee was informed that one of the key means of carrying out a fraudulent enterprise involves the creation of business or corporate entities and names that can be used as the vehicle for dishonest practices, but which will disguise the true identity of the perpetrator. Misuse of business and corporate names, as well as Internet domain names, lies at the heart of many types of fraud. For example, stolen cheques can be paid into an account opened in the name of a business that has been registered using a name nearly identical with that of the legitimate cheque payee. Often the slight discrepancy in name will not result in the cheque being returned, or the transaction queried.

In order to solve this problem the Committee has recommended establishing more stringent procedures to verify the information that individuals provide when registering businesses or incorporated associations, and when incorporating companies, or applying for domain names.

Recommendations

The Committee recommends that the procedures associated with the identification of persons who seek to register a business or incorporated association in Victoria be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of business proprietors or individuals who register an incorporated association (Recommendation 26a, p.206).

The Committee recommends that the *Business Names Act 1962* (Vic) be amended to require the Commissioner of Consumer Affairs not to register business names closely similar to existing names and likely to be confused with or mistaken for each other (Recommendation 26b, p.206).

The Committee recommends that the Attorney-General for the State of Victoria correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the identification of persons who seek to incorporate a company, to require them to provide the same evidence of identity of the person seeking incorporation as is necessary to open an account with a financial institution. The correspondence should also include a request that procedures be put in place to assist in detecting the use of false information concerning the names of directors and office bearers of companies (Recommendation 27a, p.206).

The Committee recommends that the Attorney-General for the State of Victoria also correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the choice of company names, so that company names closely similar to existing names and likely to be confused with or mistaken for each other not be registered (Recommendation 27b, p.206).

The Committee recommends that the procedures associated with the identification of persons who seek to register Internet domain names be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of registrants of domain names (Recommendation 28a, p.206).

The Committee recommends that the system of registering Internet domain names be reformed to prevent the registration of misleading domain names (Recommendation 28b, p.206).

Fraud detection

If it is not possible to prevent fraud entirely, it may at least be possible to identify the presence of fraudulent transactions quickly in order to reduce the extent of any losses suffered or the occurrence of repeat victimisation. The Committee was told of a range of measures designed to assist in the detection of fraud. These include internal detection measures, such as the use of fraud detection software, data matching and Internet usage monitoring, and external detection measures, such as the use of auditors and Internet sweeps.

The Committee heard that one of the most common ways in which fraud is detected and reported is through the use of 'whistleblowers' – people who reveal wrongdoing within an organisation to the public or to those in positions of authority. The Committee was advised, however, that some individuals fear reporting fraud because it may result in their being discriminated against or otherwise subjected to harassment, intimidation or reprisals. This is particularly the case in the private sector, where whistleblowers are provided with no statutory protection against reprisals. To overcome this problem, the Committee has recommended extending the scope of the *Whistleblowers Protection Act 2001* (Vic) to cover the private sector as well as the public sector. The Committee has also recommended that the VFIRC establish a whistleblowing 'hotline' – a telephone number that is dedicated to the reporting of relevant matters.

Due to the importance of whistleblowing as a method of fraud detection, the Committee has also recommended that the Victorian Law Reform Commission conduct an inquiry into the issue of compensating individuals for reporting fraud.

Recommendations

The Committee recommends that the *Whistleblowers Protection Act 2001* (Vic) be extended to individuals who report suspected fraud and offences involving dishonesty committed in the private sector (Recommendation 31, p.220).

The Committee recommends that VFIRC establish a hotline for reporting public or private sector fraud. It should be possible for people to report anonymously if desired. VFIRC should determine whether further investigation is required, and if so which is the most appropriate body to carry out that investigation. When providing the appropriate body with the information necessary to conduct such an investigation, care must be taken to protect the whistleblower, in accordance with the procedures set out in the *Whistleblowers Protection Act 2001* (Vic) (Recommendation 32, p.220).

The Committee recommends that the question of whether and how individuals should be compensated for reporting instances of suspected fraud should be referred to the Victorian Law Reform Commission for further inquiry. Issues to be addressed by the inquiry should include whether a fund should be established to compensate individuals who have suffered loss as a result of reporting fraud, the desirability of introducing *qui tam* laws in relation to whistleblowers, and whether scales of costs applicable to witnesses in fraud cases should be reviewed (Recommendation 33, p.220).

The Committee recommends that prior to employers monitoring their employees' use of the Internet, employees must be informed that they may be monitored, and be advised of the extent to which they can use computers for their own purposes (Recommendation 29, p.212).

The Committee recommends that a system of unique identification numbers should not be introduced at a national or state level (Recommendation 30, p.214).

Fraud reporting

The Committee heard that the primary barrier to criminal prosecution lies in encouraging those who have suffered loss at the hands of offenders to report their complaint to the authorities. As noted above, there are a variety of reasons why people tend not to report fraud, leading to a very low rate of reporting. There are two main consequences of this low reporting rate. First, it makes it impossible to understand the precise nature and extent of fraudulent activities being committed in Victoria and Australia. This makes it difficult to know exactly how this problem can best be addressed and where key risk areas lie. Secondly, it can lead to perpetrators avoiding prosecution for their acts. This not only leaves them free to commit similar acts against other individuals or organisations but also undermines the development of a culture of intolerance to fraud, which is necessary if the problem is ever to be effectively addressed.

The Committee has made a number of recommendations designed to overcome this problem. Foremost amongst these is a recommendation that all public sector agencies and private sector organisations that become aware of incidents of fraud be required to notify VFIRC within 10 working days. The Committee has recommended that VFIRC act as a clearinghouse, determining which is the appropriate agency (if any) to act upon the report, and providing that agency with the report. All reports should, however, be forwarded to Victoria Police. The Committee has also recommended making it a criminal offence to fail to report a serious offence involving dishonesty where the victim believes that any financial loss suffered would amount to at least $100,000.

Recommendations

The Committee recommends that VFIRC be the central Victorian agency to receive all reports of fraud from individuals, public sector agencies and private sector organisations (Recommendation 34a, p.231).

The Committee recommends that all public sector agencies and private sector organisations that become aware of incidents of fraud be required to notify VFIRC within 10 working days. The Committee recommends that failure to comply with this requirement be subject to appropriate sanctions (Recommendation 34b, p.231).

The Committee recommends that all public sector agencies and private sector organisations be required to notify VFIRC of the outcome of any fraud-related investigations and prosecutions within 10 working days of the outcome being known or a decision being made (Recommendation 34c, p.231).

The Committee recommends that a criminal offence be created of failure to report a serious offence involving dishonesty (being an offence within the Australian Standard Offence Classification category of dishonesty) where the victim believes that any financial loss suffered would amount to at least $100,000 (Recommendation 34d, p.231).

The Committee recommends that VFIRC act as a clearinghouse, determining which is the appropriate agency (if any) to act upon the report, and providing that agency with the report. Relevant agencies would include professional regulatory bodies such as the Legal Practice Board or the Medical Practitioners Board of Victoria, Commonwealth agencies such as the Australian Crime Commission or the Australian High Tech Crime Centre, and state agencies such as the Office of the Auditor-General or Victoria Police. VFIRC should not have any investigatory powers (Recommendation 34e, p.231).

The Committee recommends that all reports received by VFIRC be forwarded to Victoria Police. VFIRC should have the power to recommend which branch of Victoria Police (such as the Major Fraud Investigation Division or a Criminal Investigation Unit) would be most appropriate to handle the matter and to recommend that Victoria Police act in partnership with another public or private sector body, including the victim. Where the victim makes such a request, VFIRC should also be able to recommend that no police action be taken at all. Victoria Police would, however, retain final discretion in deciding how to proceed with any matter (Recommendation 34f, p.231).

The Committee recommends that VFIRC organise a forum with representatives from all appropriate agencies, to help devise guidelines for determining which agency is best placed to investigate reports that have been received (Recommendation 34g, p.232).

The Committee recommends that VFIRC produce a best practice guide to reporting fraud, including a description of what information should be provided. The guide should contain specific information on preparing reports where the matter is likely to require further police action to be taken. Similar information should be published on the VFIRC web site (Recommendation 34h, p.232).

The Committee recommends that the requirement under Direction 4.3 of the Standing Directions of the Minister for Finance, requiring cases of suspected or actual theft, irregularity or fraud under the control of their departments to be notified to the relevant Minister and the Auditor-General, be extended to all public sector agencies in Victoria including local government departments. The Auditor-General's resources should be increased to deal with any increased caseload (Recommendation 35, p.232).

The Committee recommends that all professional regulatory agencies be required to notify VFIRC of all matters involving fraud and financial crime or professional misconduct of a financial nature that come to their attention (Recommendation 2b, p.64).

Fraud investigation

In addition to the reluctance of individuals to report white-collar crime, the Committee was informed that there are many problems associated with the effective investigation of cases. White-collar crime often involves the use of highly sophisticated techniques of deception and planning, and offenders often go to considerable lengths to disguise their identity and to make documentary financial trails of evidence difficult to follow.

The Committee has made a number of recommendations to assist with internal investigations conducted by organisations themselves, as well as investigations conducted by law enforcement agencies. In particular, the Committee has recommended that Victoria Police retain primary responsibility for the investigation of fraud in Victoria, but that it should be provided with additional resources for a number of specified purposes. The Committee has also recommended the establishment of a task force to examine the policing of fraud, with a particular focus on the issue of partnership policing. The task force should aim to develop procedures that can assist law enforcement agencies to work together with the public and private sectors to build an effective fraud response framework.

Recommendations

The Committee recommends that primary responsibility for the investigation of fraud in Victoria remain with Victoria Police (Recommendation 39a, p.250).

The Committee recommends that additional resources be provided to Victoria Police to enable it to:

i. provide additional fraud-related training to its members;

ii. retain personnel with particular experience in fraud;

iii. purchase new technologies necessary to combat high tech crime;

iv. establish a new sub-division to deal with complex financial crimes that involve small-value losses which do not fall within the scope of the Major Fraud Investigation Division but are also unable to be handled by Criminal Intelligence Units owing to their complexity or the nature of the investigatory expertise required; and

v. develop clear guidelines to determine when matters will be examined by the new sub-division, the Major Fraud Investigation Division, Criminal Intelligence Units, or any other parts of Victoria Police, and when Victoria Police should work in conjunction with other state or national agencies or other bodies (Recommendation 39b, p.250).

The Committee recommends that a Ministerial Task Force be established to examine the policing of fraud, with a particular focus on the issue of partnership policing, namely the development of procedures that can assist law enforcement agencies to work together with the public and private sectors to build an effective fraud response framework (Recommendation 39c, p.250).

The Committee supports the attempt by the Australian Institute of Professional Investigators (Victorian Chapter) and the Victoria Police Major Fraud Investigation Division to draft a set of policy standards to form the basis for a national framework for all fraud investigation (Recommendation 36, p.235).

The Committee recommends that VFIRC promote the importance of private sector organisations specifying in their fraud control policies the steps to be taken in investigating suspected fraud (Recommendation 37, p.238).

The Committee recommends that public and private sector fraud control policies and investigations follow the procedures set out in the Standards Australia *Guidelines for the management of IT evidence*, to ensure that electronic evidence is preserved (Recommendation 38, p.238).

Civil and regulatory responses

When fraudulent conduct is discovered, the decision to mobilise the law, and the choice of remedy, requires that law enforcement and regulatory authorities consider a range of factors, such as the likelihood of success, the cost involved, and the public interest. The Committee heard that as an alternative, or in addition to instituting criminal action, victims of fraud may also commence civil proceedings for damages in negligence, trespass or breach of contract. To the extent that private parties have the resources and the capacity to pursue their own remedies, the limited resources of the state may be reserved for those situations where they are most sorely needed.

Victims of financial crimes may also lodge complaints with statutory licensing authorities in cases where fraud is alleged to have been perpetrated by certain professionals. The Committee was advised that although the members of the oldest professions are statutorily recognised and registered, some professionals, including accountants, are not covered by existing registration authorities, and thus are not subject to any internal professional disciplinary controls other than the potential loss of membership of a professional association. The Committee has recommended that an inquiry be conducted into the introduction of a statutory system for the professional regulation and registration of accountants, financial advisers and other financial consultants (such as mortgage brokers) who practise in Victoria, with a view to determining standards for admission to practise, and procedures for restriction of registration on proof of professional misconduct.

Recommendations

The Committee recommends that an inquiry be conducted into the introduction of a statutory system for the professional regulation and registration of accountants, financial advisers and other financial consultants (such as mortgage brokers) who practise in Victoria, with a view to determining standards for admission to practise, and procedures for restriction of registration on proof of professional misconduct. The Committee recommends that legislation governing other statutorily recognised professions in Victoria be used as a model (Recommendation 40a, p.258).

The Committee recommends that action be taken by the Australian Securities and Investments Commission to ensure that individuals who are prohibited from practising in the financial services industry are unable to circumvent such action by continuing to practise in other advisory roles (Recommendation 40b, p.258).

Criminal offences

At present in Australia each jurisdiction has its own laws and rules that regulate business and professional activities. These emanate from all levels of government, professional bodies, business organisations and many other bodies. Many are complex, unclear, and contradictory and impede the successful investigation and prosecution of many white-collar crimes. The Committee believes it is vital that any legislative response to the challenges presented by new technologies should avoid complicating matters further and attempts should be made to harmonise legal reforms across Australia as well as internationally.

The Committee heard that the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General has addressed the problem of harmonising laws in Australia, making a number of recommendations for reform in relation to dishonesty offences, including fraud and forgery. These recommendations have been adopted by the Australian government. The Committee has recommended that Victoria also adopt these recommendations, and that the *Crimes Act 1958* (Vic) be amended accordingly.

A number of other specific proposals for reform of the law were suggested to the Committee, such as the creation of specific identity-related fraud offences offences. While some of these proposals clearly had merits, the Committee has recommended that Victoria refrain from undertaking such specific legislative reform, instead referring the identified problems for resolution on an Australia-wide basis.

Recommendations

The Committee supports continuing attempts to harmonise nationally the law relating to fraud and other dishonest conduct, including crimes involving misuse of identity and dishonest practices relating to payment cards and electronic payment systems (Recommendation 41, p.265).

The Committee recommends that the *Crimes Act 1958* (Vic) be amended to reflect the recommendations of the Model Criminal Code Officers Committee in relation to dishonesty offences, including fraud and forgery, as enacted in Divisions 133-137 and 143-145 of the *Criminal Code Act 1995* (Cth). In amending the law, it should be ensured that:

i the means of proving dishonesty in Victoria be determined according to the standards of ordinary people, and known by the accused to be dishonest according to those standards;

ii. the definition of 'property' that can be fraudulently obtained includes intellectual property and computer data;

iii. company directors and employees can be charged with the relevant offences where they have defrauded their own company;

iv. people can be charged with the relevant offences where they have defrauded a pooled fund;

v. offences are applicable to fraud committed in an online environment; and

vi. Victorian fraud and dishonesty-related offences be able to be charged in any case where the offence was committed in Victoria, or where the victim was in Victoria at the relevant time (Recommendation 42, p.265).

The Committee recommends that a general fraud offence should not be established in Victoria (Recommendation 43, p.265).

The Committee recommends that the development of a national legislative response to questions of theft of identity, identity-related fraud and credit card fraud including card skimming and the possession of equipment or devices used in connection with credit card fraud be referred to the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General for investigation and report. In doing so, consideration should be given to:

i. The introduction of an offence of assuming a false identity with the intention to commit a serious offence;

ii The introduction of offences proscribing the possession of equipment or devices (including plastic cards), with intent to dishonestly counterfeit or alter documents or to assist in the commission of an offence involving dishonesty;

iii. The introduction of offences proscribing the importation, possession and use of equipment or devices (including plastic cards), with intent to dishonestly obtain funds through the deception or manipulation of payment systems; and

iv Reversing the onus of proof (Recommendation 44a, p.273).

The Committee recommends that criminal offences relating to theft of identity, identity-related fraud or credit card fraud should not be implemented until a national approach to these issues has been agreed upon (Recommendation 44b, p.273).

The Committee recommends that any new criminal offences relating to theft of identity, identity-related fraud or credit card fraud should be technology-neutral (Recommendation 44c, p.273).

The Committee supports national initiatives designed to reduce the incidence of unsolicited email ('spam') (Recommendation 45, p.280).

Procedural issues

Once a case of white-collar crime has been investigated it then remains for evidence to be presented to the relevant prosecution agency. The Committee was informed of a number of problems that can arise at this stage. These include problems with the sufficiency of evidence, the length of trials, and the complexity of cases.

A number of strategies have been adopted to address these issues. Legal practitioners are now closely regulated with respect to the length, manner and nature of material they present to the courts. The use of 'directions hearings' in criminal trials seeks to ensure that criminal proceedings go ahead

appropriately and promptly through interlocutory stages, while mechanisms are in place that aim at the early resolution of factual disputes. Computer technology has also greatly facilitated the presentation and analysis of complex business dealings. Despite such measures, however, continuing dissatisfaction with the criminal justice process was expressed to the Committee by numerous parties.

To address some of these concerns, the Committee has recommended the establishment of specialist fraud lists in the Supreme and County Courts. The Committee has also recommended the provision of additional funding to the courts, to enable greater use to be made of computer technologies. The Committee does not, however, support the introduction of specialist juries, panels of assessors or trial by judge alone.

Recommendations

The Committee recommends that juries continue to be the appropriate body to make factual determinations in cases involving fraud and dishonesty-related offences. The Committee does not support the introduction of specialist juries, panels of assessors or trial by judge alone (Recommendation 47, p.291).

The Committee recommends that there should be specialist fraud lists in the Supreme and County Courts (Recommendation 48, p.291).

The Committee recommends that additional funding be allocated to the improvement of courtrooms in Victoria to enable information to be provided to judges, lawyers and members of juries electronically through the use of computers and displayed on screens in courtrooms during proceedings (Recommendation 49, p.291).

Sentencing

The extent to which severe sentences should be used for fraud offences has been subject to considerable debate over the years. Some of those who provided evidence to the Committee argued that sentences imposed on white-collar criminals are inadequate, while others expressed doubts as to whether severe sentencing had any real deterrent effects. The Committee has examined this issue in some detail in the Report. In the interests of national harmony, the Committee has recommended that maximum penalties for fraud and deception-related offences be consistent with those set out in the *Criminal Code Act 1995* (Cth).

Recommendation

The Committee recommends that maximum penalties for fraud and deception-related offences be consistent with those set out in the *Criminal Code Act 1995* (Cth) (Recommendation 50, p.298).

Victim support services

The Committee received a number of submissions concerning the desirability of support services being provided for the victims of financial crimes. The argument was raised that the services provided by victim support agencies, which have traditionally focused on the victims of violent crime, need to be extended to the victims of economic and white-collar crime as well. In particular, the Committee heard that specialist victim support services are needed for those who fall prey to identity fraud offenders, as often complex procedures are required to reinstate one's credit rating after it has been destroyed through the acts of an identity thief.

The Committee has recommended that VFIRC be the central agency within Victoria responsible for co-ordinating support services for victims of fraud-related offences and their families, including victims of identity theft. The Committee believes that procedures should also be developed to assist victims of identity theft to recover any loss or damage sustained as a result of the theft, including restoration of their credit rating.

Recommendations

The Committee recommends that VFIRC be the central agency within Victoria responsible for co-ordinating support services for victims of fraud-related offences and their families, including victims of identity theft (Recommendation 51a, p.299).

The Committee recommends that procedures be developed to assist victims of identity theft to recover any loss or damage sustained as a result of the theft, including restoration of their credit rating. Consideration should be given to:

i. the development of a formal certificate (with appropriate security) outlining the name of the victim and the offence, which could be used to prove that they have been the victim of a crime; and

ii. the development of a standard affidavit for victims of identity crimes to be used by victims trying to counter the effects of identity theft, alleviating the need for filling out multiple forms (Recommendation 51b, p.299).

The Committee recommends that VFIRC provide information to victims of identity theft, including steps that can be taken to recover any loss or damage sustained as a result of the theft (Recommendation 51c, p.299).

Education

The Committee believes that effective education is one of the most important fraud control measures. Both management and staff of organisations need to be educated about the risks of fraud and about organisational measures that can help to prevent fraud from being committed. Members of the community also need to be educated about the types of activities to which they are most vulnerable, the most appropriate means of prevention, and the best avenues of

response when they believe they have been victimised. In particular, there is a need to enhance knowledge of dishonest criminal activities among those at the greatest risk of being defrauded, such as young people who may use new technologies without giving sufficient consideration to the risks of fraud, and some older persons who may be targeted as potentially susceptible victims.

At present there is a considerable amount of such information available. The Committee heard of a number of organisations and web sites that provide advice about fraud-related matters. It appears to the Committee that people seeking guidance in the area may actually suffer from information being disseminated through too many avenues. This can be confusing, particularly given the different ways in which fraud is dealt with in different jurisdictions. In addition, many of these sites focus on specific elements of fraud, such as Internet or electronic commerce-related fraud, rather than providing an overview of fraud in general. This can necessitate visiting a variety of web sites in order to obtain comprehensive information.

To address this problem, the Committee has recommended that VFIRC become the central Victorian agency responsible for providing information to the public and private sectors in relation to fraud. VFIRC would be a 'one-stop shop' for all fraud-related matters in Victoria. This role of VFIRC should be widely promoted, so that any organisations or individuals seeking fraud-related information would know that their first step should always be to contact VFIRC.

The Committee has also recommended the development of an informal forum, within which fraud-related matters can be discussed by those people required to handle such matters in the course of their employment.

Recommendations

The Committee recommends that VFIRC be the central Victorian agency responsible for providing information to the public and private sectors in relation to fraud prevention matters (Recommendation 22a, p.196).

The Committee recommends that, in addition to the activities outlined in the recommendations above, VFIRC conduct the following fraud prevention activities:

i. Carry out programs designed to inform the business community and individuals in Victoria of the risks of fraud and electronic commerce-related crime and of the fraud prevention measures that can be used to minimise the risk of victimisation. This should include a mail-out to all Victorian households of an information brochure on prevention methods that could be used to reduce the risk of fraud victimisation in consumer transactions, business transactions, and electronic transactions, highlighting the importance of the responsible maintenance of passwords and PINs;

ii. Conduct training sessions and/or seminars in relation to fraud control (including information security management), as well as encouraging public and private sector agencies to disseminate and explain their fraud control policies widely amongst staff and periodically hold in-house fraud prevention training. In particular, where staff are required to verify documents used to establish identity, organisations should be encouraged to train them in identifying counterfeit and altered documents;

iii. Develop best practice guidelines to help organisations implement authentication systems (including password management systems) appropriate to their security needs; and

iv. Develop a web site containing fraud prevention information for the public and private sectors and for individuals (Recommendation 22b, p.196).

The Committee recommends an informal fraud prevention and control network, such as the New South Wales Corruption Prevention Network, be established in Victoria. Steps should be taken to facilitate the establishment of such a network, including the provision of seed funding if necessary. The existence of the network should be promoted by VFIRC (Recommendation 23, p.199).

Further research

Although considerable research has been undertaken to document the nature and extent of fraud in Victoria, the Committee believes that there remains a need for further specifically targeted research activities. For example, the Committee believes that annual surveys should be conducted of businesses and companies operating in Victoria to determine the nature and extent of their fraud and electronic commerce-related victimisation. In addition, a comprehensive study should be undertaken in Victoria to determine the financial and indirect costs associated with fraud and electronic commerce-related crime in Victoria.

Research is also needed to examine specific areas of risk. The Committee has identified both the higher education sector and the gambling industry as worthy of further investigation. These areas could provide environments that create opportunities for crimes of dishonesty to occur (in the case of higher education) or to lead to the indebtedness of their patrons (in the case of gambling venues), which may result in the commission of financial crime. Further research should also be conducted in the area of asset confiscation, to see whether Victorian courts should be given the power to freeze property at the request of a foreign state while forfeiture proceedings take place in their jurisdiction.

Recommendations

The Committee recommends that surveys be conducted of businesses and companies operating in Victoria to determine the nature and extent of their fraud and electronic commerce-related victimisation (Recommendation 5a, p.91).

The Committee recommends that a study be undertaken in Victoria to determine the financial and indirect costs associated with fraud and electronic commerce-related crime in Victoria (Recommendation 5b, p.91).

The Committee recommends that research be undertaken to determine the nature, extent and financial cost of fraud perpetrated in the higher education sector in Victoria (including Tertiary and Further Education Institutes), and steps which can be taken to address this problem (Recommendation 5c, p.91).

The Committee recommends that research be undertaken to ascertain the links between fraud and gambling, and ways in which this issue can be addressed (Recommendation 5d, p.91).

The Committee recommends that the issue of whether Victorian courts should be given the power to freeze property at the request of a foreign state while forfeiture proceedings take place in their jurisdiction be further investigated (Recommendation 46, p.283).

Changing attitudes

Finally, the Committee has formed the view that the effective prevention of fraud should entail the development of a culture of intolerance to conduct of this nature throughout the community. Deceptive and manipulative practices, in whatever walk of life, should not be condoned. Constructive education campaigns, such as those used to help change attitudes about discriminatory practices in the community, could be employed throughout Victoria, and indeed Australia, to explain why dishonest and corrupt practices are unacceptable. Substantial resources may need to be allocated for achieving generalised changes of attitudes, from both public and private sectors, although compelling evidence exists to indicate that expenditure on such initiatives would be cost-effective in reducing losses sustained through white-collar crime.

The Committee heard that fraud is always going to be a risk of modern life, and that as technology continues to develop, particularly with respect to online commercial activities, increasingly large amounts will be misappropriated from both individuals and organisations. Although fraud and white-collar crime are often perpetrated using complex strategies to trick unsuspecting individuals into parting with money, and even more complex means to disguise the proceeds of dishonest activities, some of the most effective means of preventing such activities are often relatively simple and

within the reach of everyone. The Committee believes that the information derived from its extensive inquiry into fraud and electronic commerce will provide a sound basis for enabling all Victorians and all Victorian organisations to understand the fraud risks which they face and how best to guard against them.

Contents

Appendices

List of Tables and Figures

Tables

Figures

Acknowledgments

This Final Report incorporates, with permission, material previously published as Smith, R.G. 2002, 'White-collar Crime', in Graycar, A. and Grabosky, P. (eds.), *The Cambridge Handbook of Australian Criminology*, Cambridge University Press, Cambridge, pp.126–56; 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; and Smith, R.G. and Grabosky, N. 1998, *Taking Fraud Seriously: Issues and Strategies for Reform*, Institute of Chartered Accountants in Australia, Fraud Advisory Council, Sydney.

Additional research on refund fraud and business fraud was undertaken by Ms Jessica Marshall, formerly Research Assistant at the Australian Institute of Criminology.

Statistical information in Appendix E was provided by Victoria Police Statistical Services Division.

Library services were provided by the Australian Institute of Criminology's J. V. Barry Memorial Library (Ms Janet Smith, Mr John Myrtle, Ms Joy Cocker and other staff), the Victorian Office of the Correctional Services Commissioner's Resource Centre (Mr Malcolm Feiner), and the Parliament of Victoria Library (Ms Debra Reeves and Mr Jon Brenkel).

Mignon Turpin has assisted the Committee in editing the Report and Chris Watson from zapwhizz.com.au has designed and laid out the contents of the Report, and Matt Clare from Mono Design designed the Cover.

List of Abbreviations

ABA	Australian Broadcasting Authority
ABCI	Australian Bureau of Criminal Intelligence
ABR	Australian Business Register
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACFE	Association of Certified Fraud Examiners
ACPR	Australasian Centre for Policing Research
ADMA	Australian Direct Marketing Association
AFC	Australian Fraud Centre
AGEC	Action Group into the Law Enforcement Implications of Electronic Commerce
AHTCC	Australian High Tech Crime Centre
AIPI	Australian Institute of Professional Investigators
ANAO	Australian National Audit Office
ANCO	Australian National Classification of Offences
APS	Australian Public Service
AS	Australian Standard
ASC	Australian Securities Commission
ASIC	Australian Securities and Investments Commission
ASOC	Australian Standard Offences Classification
AUSTRAC	Australian Transaction Reports and Analysis Centre
CCLG	Corporate Crime Liaison Group
CIU	Criminal Investigation Unit
CII	Council of International Investigators
CPN	Corruption Prevention Network
DSS	Department of Social Security
EBT	Electronic Benefits Transfer
EMV	European Mastercard Visa
ESCG	E-Security Co-ordination Group
FICC	Financial Institutions Consultative Committee

FMCF	Financial Management Compliance Framework
FMP	Financial Management Package
HIC	Health Insurance Commission
IAFCI	International Association of Financial Crimes Investigators
IFCC	Internet Fraud Complaint Center
IIA	Internet Industry Association
ISA	International Standard of Auditing
ISP	Internet Service Provider
LEAP	Law Enforcement Assistance Program
MFID	Major Fraud Investigation Division
NIST	National Institute of Standards and Technology
NOIE	National Office for the Information Economy
OECD	Organisation for Economic Cooperation and Development
SAIA	South Australian Internet Association
SIRCA	Securities Industry Research Centre for the Asia-Pacific Ltd
VFIRC	Victorian Fraud Information and Reporting Centre
VLRC	Victorian Law Reform Commission
VPS	Victorian Public Service
WAIA	Western Australian Internet Association

1. Introduction

Fraud and white-collar crime have far-reaching effects on the community, not only in terms of the financial impact on business and government, but also because of the effects on individuals who are victimised. On many occasions these individuals suffer substantial hardship and personal consequences and yet often the offences are seen as less serious than ordinary street crime. In giving evidence to the Committee Honourable Justice Frank Vincent observed:

> One of the things that intrigues me is this: there is a suggestion that regularly intrudes into these kinds of discussions that these people are somehow nicer than other criminals. If a man breaks into your house and steals your television set, you do not tend to be terribly sympathetic, but very frequently we are encountering individuals who have destroyed lives and futures and aspirations, who have done on occasions damage to the very economies of the states in which they have been operating.[1]

As will be discussed later in this Report, fraud is estimated to have cost Victoria as much as $641 million last year – money which could be better used for essential community works in promoting health, education and security.

In recent years fraud has increasingly involved the use of electronic communications and computing technologies that support so-called electronic commerce. Risks of fraud associated with these technologies have, arguably, retarded the development and implementation of electronic commerce globally (see, for example, Grabosky, Smith & Dempsey 2001; Smith & Urbas 2001).

It is the purpose of the present Inquiry to examine the trends in this area and to look at how Victorian law and policy can deal with these wide-ranging issues. By reviewing the topic and identifying key issues for discussion, the present study will help to ensure that Victoria's response reflects best practice and is in accord with measures implemented in other places in response to these global concerns.

---

1 Hon. Justice Frank Vincent, Justice of the Supreme Court of Victoria, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 November 2003.

The current Inquiry

On 28 November 2001, the Victorian Legislative Assembly referred the following Terms of Reference to the Drugs and Crime Prevention Committee:

> To the Drugs and Crime Prevention Committee – for inquiry, consideration and report by 30 September 2002 on:
>
> (a) the extent and nature of fraud and white-collar crime in Victoria;
>
> (b) the impact of new technology supporting E-commerce on the opportunities for fraud;
>
> (c) the current and proposed state, Commonwealth and international strategies and initiatives in relation to dealing with fraud and white-collar crime; and
>
> (d) the need for policy and legislative reform to combat fraud and white-collar crime in Victoria.

Following discussions concerning the scope of the Inquiry, the Minister for Police and Emergency Services requested that the Committee focus, in particular, on definitional issues, emerging trends and best practice responses to instances of fraud and electronic commerce-related crime in Victoria.

On 30 October 2002 the Committee released *Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses – Discussion Paper*. This Discussion Paper outlined the nature and extent of fraud in Victoria, with a particular focus on the fraud risks of electronic commerce. Some possible avenues for reform were raised, and a number of questions were posed. The public was invited to make written submissions by 30 January 2003.

On 5 November 2002 the 54th Parliament was prorogued, causing the Inquiry to lapse. On 17 April 2003, however, the Governor in Council reissued the same terms of reference to the Drugs and Crime Prevention Committee of the 55th Parliament with a requirement to report to Parliament by 31 December 2003. The deadline for written submissions was subsequently amended to 7 July 2003. Sixteen written submissions were received from a variety of organisations and individuals.[2]

In addition to receiving written submissions, the Committee has undertaken an extensive review of the literature in the area, as well as having attended a number of seminars and conferences.[3] The Committee has also travelled interstate to gain information. Meetings were held with key government and non-government agencies in Canberra, Sydney, Brisbane, Perth and Adelaide to discuss approaches to fraud.[4] Public hearings were also conducted in

2 For a list of the submissions received by the Committee see Appendix A-1.

3 For a list of seminars and conferences attended see Appendix A-2.

4 For a list of interstate meetings and site visits see Appendix B-1.

Melbourne on 4 and 15 September 2003, on 6 October 2003 and on 7 November 2003.[5] In total, the Committee received oral evidence from 61 witnesses.

Definitional issues

White-collar crime

The definition of white-collar crime has been an enduring topic of debate throughout the twentieth century (see Smith 2002b and the extensive review of definitions of white-collar crime conducted by Geis 1991). It has been observed that white-collar crime is 'a social rather than a legal concept, one invented not by lawyers but by social scientists' (Weisburd, Wheeler & Waring 1991, p.3). There is no specific offence or group of offences that can be identified as white-collar crime (Freiberg 1992). As such, using white-collar crime as a concept with which to discuss policy and legal reform presents some difficulties.

The traditional definition of white-collar crime focused on crimes committed by persons of high status and social repute in the course of their occupation (Sutherland 1940). Included in this definition were crimes committed by company officers, public servants, and professional people such as doctors and lawyers. The original emphasis was on economic crime (that is, crimes in which financial gain is the principal objective), although over time white-collar crime has come to include any acts of occupational deviance involving a breach of the law or ethical principles. As such, white-collar crime now includes almost any form of illegality other than conventional street crimes (Freiberg 1992).

Technological developments over the last decade have, however, created further complexities surrounding the types of persons that are able to commit white-collar crime. The perpetrator of an online fraud, for example, might just as easily be a self-taught teenager using a personal computer at home as a professional person in the workplace.

Not all offences perpetrated by white-collar criminals involve a breach of the criminal law, as there are numerous regulatory, ethical and civil misdemeanours that some people argue should be included within the definition of white-collar crime. Conversely, certain offences of great relevance to this Inquiry, such as welfare or credit card fraud, would be excluded using a traditional definition of white-collar crime (Braithwaite 1985).

The essence of white-collar crime, however, remains rooted in abuse of power and breach of trust, usually involving the pursuit of financial gain as a motive. A simple categorisation of white-collar crime distinguishes crimes committed by specified types of offenders (mainly professionals and individuals employed by corporations) from crimes perpetrated in specified ways (mainly economic

5 For a list of witnesses who gave oral evidence to the Committee at meetings or public hearings see Appendix B-2.

crimes that involve sophistication, planning, or the use of technology in their commission).

Corporate crime

Perhaps the clearest conception of white-collar crime is that which arises out of corporate activities – although even here there are a number of ways in which corporate crime can be defined (Smith 2002b). Tomasic (1993), for example, proposed a fourfold classification:

- corporate crime committed by a corporation itself for the benefit of that corporation;
- corporate crime committed by the agents or controllers of a corporation for the benefit of that corporation;
- corporate crime committed by a corporation itself against the interests of another corporation; and
- corporate crime committed by the agents or controllers of a corporation against the interests of the corporation.

Examples of corporate crimes and other forms of corporate illegality include infringements of the Corporations Law, taxation offences, non-compliance with occupational health and safety and anti-discrimination legislation, breaches of environmental protection laws, consumer protection offences relating to deceptive practices and the sale of dangerous or unhealthy products, infringements of trade practices and competition legislation, intellectual property crimes, bribery and corrupt practices in dealing with government agencies, and various economic offences concerning employees, such as breaches of industrial awards and non-payment of wages and superannuation (Grabosky 1984).

In an attempt to limit the scope of the present Inquiry, this Report does not deal with corporate criminal liability, which has recently been examined in depth by Clough and Mulhern (2002).

Fraud and dishonesty

Although not specifically defined by legislation in Victoria, fraud is a generic category of conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage over another person or entity. Australian Auditing Standard AUS 210 defines fraud as 'an intentional act by one or more individuals among management, those charged with governance of an entity, employees, or third parties involving the use of deception to obtain an unjust or illegal advantage' (Auditing and Assurance Standards Board 2002).

Both criminal sanctions and civil remedies may apply to such conduct and sometimes both at once, although in this context it is the criminal species of fraud that is at issue. As Lanham, Weinberg, Brown and Ryan observe:

> Criminal fraud is one of the besetting evils of our time. While less dramatic to individuals than crimes of violence like murder, rape and wounding, fraud can still at the individual level inflict misery and hardship. At the community level the damage is immense, involving as it does many millions of dollars (Lanham et al. 1987, p.vii).

Yet even criminal fraud appears in many guises, not all involving financial consequences. For example, section 57 of the *Crimes Act 1958* (Vic) contains the offence of procuring sexual penetration by threats or fraud. This makes fraud a difficult concept to delineate. An indication of the far-reaching scope of fraud is apparent from Appendix C-1 which sets out 137 deception offence descriptions currently used in Victoria Police statistics. Appendix C-2 sets out a further 170 offence descriptions that could also be relevant to the prosecution of certain other forms of fraud and dishonesty, including conduct that relates to electronic commerce. The complex nature of this area of law, even without the additional layer of issues raised by electronic commerce, is one of the main challenges facing reformers.

The law concerning fraud and dishonesty consists of a patchwork of statute, both state and Commonwealth, and the common law. It is so complex that according to the authoritative text on the topic, 'any attempt to cover the whole of the law relating to criminal fraud in Australia would require an encyclopedia' (Lanham et al. 1987, p.vii). Indeed, as suggested by the number of fraud-related offences noted above, the Victorian law in this area is formidable in its own right.

At the heart of all fraud, however, lies the concept of dishonesty, and it is the dishonest gaining of property and financial advancement using the technologies and infrastructure supporting legitimate electronic commerce that serves as the focus of this Inquiry. The interpretation of dishonesty has been debated constantly since the English *Theft Act* brought it to prominence (see for example Elliott 1980; Williams 1999b; Steel 2000).

Dishonesty is the key attribute that distinguishes fraudulent from innocent conduct. Rather than define dishonesty in legislation it is usually a matter of fact for juries to determine in criminal cases. Section 130.3 of the Commonwealth *Criminal Code Act 1995*, for example, defines dishonest as:

> (a) dishonest according to the standards of ordinary people; and
>
> (b) known by the defendant to be dishonest according to the standards of ordinary people.

The key issue in determining dishonesty is the intention of the individual involved. The unauthorised destruction of a computer file may not necessarily be fraudulent in the financial sense (it could, for example, be an act of vandalism) but if the same action were carried out with an intention to destroy specific evidence of a contractual obligation and thereby avoid a loss, then fraud may be involved. The physical aspect of fraud, therefore, is singularly incapable

of exhaustive definition. As the issue of fraud in the new context of electronic commerce is confronted, it is as well to recall Lord Hardwicke's observation, written in 1759, that:

> Fraud is infinite, and were a court of equity once to lay down rules, how far they would go, and no farther, in extending their relief against it, or to define strictly the species of evidences of it, the jurisdiction would be cramped, and perpetually eluded by new schemes which the fertility of man's invention would contrive (quoted in Page 1997, p.292).

This line of argument has been used to argue for a general fraud or dishonesty offence, which would be applicable regardless of the particular means used (Page 1997).

In medieval times, the law took the view that 'the thought of man is not triable', hence the state of mind of the accused was not regarded as a suitable subject of inquiry for the courts (Page 1997, p.289). 'Larceny', the prototype common law offence from which all theft and fraud offences subsequently grew, was originally confined to physical taking of items by force or stealth. Instances of the taking of property through trickery or abuse of one's position were classified as torts, that is, civil wrongs. The gradual expansion of the criminal law to encompass increasingly abstract and subtle property offences is a process that continues today, and now the state of mind of the accused is at the very centre of the offences with which this Report is concerned.

Electronic commerce

Electronic commerce encompasses a wide range of activities, however it essentially involves the use of computing and communications technologies to advertise, trade in and pay for goods and services.

Various technologies can be used for electronic commerce including electronic mail, facsimile transfers, and a variety of web-based systems for the sharing and exchange of information. Acts of dishonesty, deception and misrepresentation relating to any of these technologies are included within the scope of this Inquiry.

Examples include sending misleading and deceptive information to a business or government agency, manipulating electronic payment systems, misappropriating corporate information and intellectual property from the Internet, identity-related deception when using the Internet, failing to honour commercial obligations entered into electronically, and using misleading domain names with intent to defraud. Also included are acts of dishonesty that make use of online business communications, business and government bulletin boards, electronic mail and the World Wide Web (Smith & Urbas 2001).

In the world of electronic commerce, a variety of short-hand expressions have been devised to characterise various types of transactions. These include B2B – business to business; B2C – business to consumer; B2G – business to government; and P2P – person to person. Throughout this Report these

expressions will generally be avoided as their definition and scope is often unclear and their use can be confusing. Addressing so-called B2G issues should include not only communications sent from business entities to government agencies, but also communications sent from government agencies to businesses, which sometimes raise problems distinct from the former category of communications. In addition, describing businesses as the source of communications also neglects the distinction between corporate entities, registered unincorporated associations, partnerships and other business models (see Smith & Urbas 2001).

As is the case with fraud and white-collar crime, there is no simple statutory offence in relation to misusing electronic commerce for financial gain. Conduct of this nature may be prosecuted as theft or dishonesty offences, misleading advertising offences under consumer affairs and trade practices legislation, infringements of Commonwealth telecommunications and financial services legislation, or Commonwealth and state computer crime offences. These offences will be considered in more detail in Chapter 10).

The focus of this Report is on those acts of dishonesty that are motivated by financial gain. Clearly, in the online era there are endless opportunities for 'electronic fraud' in the form of plagiarism (passing off another's work as one's own), although this may only rarely be attributable to a financial motive. Equally, a wide conception of electronic commerce-related crime could involve issues such as the disruption of systems through vandalism that occurs when viruses disable computers, or crimes involving the dissemination of objectionable or illegal material, such as when businesses or individuals seek to sell child pornography online. However, such crimes do not form a part of the present Inquiry unless they involve some element of deception or dishonesty in which the perpetrator is seeking to obtain a financial gain.

The phenomenon of electronic commerce challenges our conventional distinction between the public and private sectors, and many of the issues raised in this Report will be shared by business and government alike. Multimedia Victoria has described part of the impact of electronic service delivery as follows:

> It is therefore possible that all information in electronic form which contemplates exchange of value will fall within the ambit of electronic commerce. Electronic commerce embraces all such agreements bearing a trading or commercial character, most notably in the form of sales, sponsorships, leases and licences. The electronic delivery of government services, such as online registrations and tenders, changes of address and electoral enrolments (which may not always be considered commercial in a conventional sense), assumes a commercial character when supplied via the Internet (Multimedia Victoria 1998, p.7).

An inescapable consequence of the nature of electronic commerce is that policy solutions are most likely to be effective when devised and implemented on a basis of co-operation between stakeholders. This means co-ordination and co-

operation between local, state, national and supranational levels of governance and law enforcement, as well as corporate entities and other parties concerned. No one party, acting alone, can expect to be able to tackle electronic fraud effectively.

Other inquiries in Australia and overseas

Throughout Australia an extensive number of organisations and individuals are involved in attempts to minimise risks of fraud that is perpetrated both conventionally and electronically. There have been numerous reviews of fraud and its control at both a state and territory level, as well as federally. Suggested responses to the problem of electronic fraud principally have a national focus, in view of its ability to be committed across borders and the need to harmonise control measures across jurisdictions. The existence of so much interest in the problem has, however, led to some incidence of duplication of effort, with one individual commenting to the Committee during its meetings that the response to fraud was something of 'a travelling circus'.[6] There is, accordingly, a need for a holistic, unified, whole-of-government approach to fraud control, especially in relation to crimes committed electronically.

In relation to fraud control, the private sector has played a leading role in conducting inquiries and in devising appropriate responses. In 1998, for example, the Fraud Advisory Council of the Institute of Chartered Accountants in Australia (Smith & Grabosky 1998) published its report *Taking Fraud Seriously: Issues and Strategies for Reform*, which provided a comprehensive review of the problem of financial crime in Australia and the ways that both public and private sector agencies were responding to it. This leading report provided the impetus for a number of subsequent investigations and responses.

The Australian Bankers Association has established a Fraud Task Force which has sought to co-ordinate the fraud control activities of major financial institutions across Australia.[7] Although there have been some achievements in this area, there remains a need for a co-ordinated response to fraud control within the financial services sector. One possibility would be the development of national bank fraud statistics and trend information, similar to that which has been gathered for many years now by the British Bankers Association and the Association for Payment Clearing Services in Britain. These organisations collect and publicly disseminate information on the nature and extent of fraud in relation to payment systems throughout England and Wales. Similar transparency does not occur in Australia, making it impossible to know precisely how much fraud exists in the financial services sector.

6 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, 25 June 2003.

7 Ms Liz Atkins, Australian Transaction Reports and Analysis Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

In the area of financial planning and stock broking, an investigation is currently being conducted by a group of independent researchers based upon information obtained from the Australian Securities and Investments Commission, which should be of use in understanding the nature of dishonesty committed by those operating within this sector.[8]

Private sector associations of financial crimes investigators have also shown a high level of commitment to responding to the problem of fraud. Groups such as the International Association of Financial Crimes Investigators (IAFCI), the Council of International Investigators (CII), and the Association of Certified Fraud Examiners (ACFE), each of which has membership in Australia, hold regular meetings in which members share information on fraud control and the latest approaches to investigation of financial crime. IAFCI, for example, is a non-profit organisation made up of law enforcement officers and investigators who collect and exchange information about fraud. Its membership includes credit card issuers, financial institutions, postal services and others with an interest in the financial services sector. IAFCI has approximately 8,000 members globally with three Chapters in Australia (including Victoria, which covers Tasmania, South Australia and Western Australia, another in Queensland and an Australia-Asia/Pacific chapter which covers New South Wales, Canberra and Asian-Pacific countries, including New Zealand). It meets bi-monthly to discuss key topical issues such as identity fraud risks and the latest technological solutions, such as computer chip cards.[9]

In Victoria, the Australian Institute of Professional Investigators (AIPI) has a similar function of enabling professionals working in the area of financial crime investigation to share information of local interest. On 1 July 2003, AIPI merged with the Corporate Crime Liaison Group and the merged body (AIPI (Victoria Chapter)) now has a membership in Victoria of over 150 Melbourne-based accountants, lawyers, police officers, other government law enforcement and regulatory officers and corporate investigators. This body is the pre-eminent body for fraud investigators in the Victorian business community, and provides a forum for networking and exchange of information.[10]

In order to facilitate the exchange of information between public and private sector investigators, the Financial Institutions Consultative Committee (FICC) exists in Victoria as an initiative of Victoria Police, Major Fraud Investigation Division, to facilitate discussion between financial institutions, fraud investigators, and law enforcement agencies.[11] Regular meetings are held in Melbourne at which topical issues are discussed by specialists.

---

8 Mr Tim Farrelly, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

9 Mr Bruce Cox, Regional Director Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003.

10 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

11 Prior to 1 January 2003 the Major Fraud Investigation Division was known as the Major Fraud Group.

There is also a wide range of initiatives taking place at the federal level to deal with fraud and E-commerce risks. The Australian Government Attorney-General's Department has recently revised its Fraud Control Guidelines which now provide a comprehensive set of principles for federal public sector agencies to follow (see discussion in Chapter 5). Of particular importance are the revised reporting requirements for agencies contained in the policy, which should enable the extent of fraud victimisation at the federal level to be more easily and accurately quantified. The policy also enshrines principles for dealing with fraud reporting and sets out uniform risk assessment and risk management procedures. The Attorney-General's Department has also undertaken research into the problem of identity fraud in the form of a comprehensive paper *Scoping Identity Fraud* presented in 2001.

In 2000 the House of Representatives Standing Committee on Economics, Finance and Public Administration conducted a comprehensive review of the Australian National Audit Office's (ANAO) Report on the Management of Tax File Numbers, entitled *Numbers on the Run*. The ANAO Report found, amongst other things, that there were 3.2 million more Tax File Numbers than the number of Australians, thus indicating potential misuse of identity for financial crime. Various recommendations were made as to how the problem could be addressed, a number of which have been implemented. The Australian Taxation Office, for example, is working with federal and other agencies to agree on protocols to enhance procedures for verifying primary documents in connection with income taxation procedures. The Tax File Number Improvement Project is also focussing on identity-related fraud.[12]

The House of Representatives Standing Committee on Legal and Constitutional Affairs has also been conducting an Inquiry into Crime and the Community: Victims, Offenders and Fear of Crime, part of which included an examination of fraud risks for Australians and how best to respond to them. This Committee is yet to produce its Final Report (see http://www.aph.gov.au/house/committee/laca/crimeinthecommunity/inqinde.htm).

The Australian Crime Commission (ACC) also has an interest in nationally significant financial and other crime from an intelligence-led law enforcement perspective. Following its establishment on 1 January 2003, the ACC has maintained the National Fraud Desk which includes identity fraud registers that record details of persons suspected of involvement in identity fraud incidents and recent methodologies. The National Fraud Desk also disseminates information on current fraud trends, fraud alerts and other information for federal, state and territory law enforcement agencies.

In 2002 the Australasian Centre for Policing Research (ACPR) prepared a scoping paper for Police Commissioners and developed the Australasian Identity Crime Policing Strategy, which was endorsed in 2003 by the

12 Mr Chris Barlow, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

Australasian Police Ministers Council. The ACPR is further analysing the problem of identity crimes from a policing perspective and will maintain this reference until 2006. The Police Commissioners Identity Crime Policing Strategy and the Electronic Crime Strategy are key initiatives in the policing response to crimes that relate to the technologies that support electronic commerce.[13]

Two other initiatives that relate to electronic crime are the establishment of the Australian High Tech Crime Centre (AHTCC) and the work of the Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC), chaired by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

The AHTCC commenced operation early in January 2003 and provides a national response to electronic crime, with resources drawn from each state and territory police service. The Centre is based at the offices of the Australian Federal Police in Canberra but has responsibility for assisting in all types of high tech crime. Recently, for example, it has been involved in the investigation of cases of plastic card skimming.[14]

The AGEC includes representatives from the Australian Federal Police, the Australian Crime Commission, the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, the Australian Government Attorney-General's Department, the Department of Immigration, Multicultural and Indigenous Affairs, the Australian Competition and Consumer Commission, the Australian Customs Service, the Australian Taxation Office, and the federal Director of Public Prosecutions, with other agencies as observers. It aims to provide a comprehensive and cohesive law enforcement and regulatory agency contribution to the Australian Government's electronic security strategic objective of creating a secure and trusted electronic operating environment. It identifies issues, develops policy and raises awareness of security issues relating to electronic commerce. The AGEC also attempts to work closely with industry bodies, such as the Internet Industry Association, to assist in its dealings with electronic fraud, and to assist law enforcement with the information needed to investigate and prosecute those crimes.[15]

AUSTRAC has also maintained a Working Party on Proof of Identity for a number of years, and in 2002 it engaged consultants – the Securities Industry Research Centre for the Asia-Pacific Ltd (SIRCA) – to estimate the cost of

13 Mr Des Berwick, Executive Officer, Australasian Centre for Policing Research, in conversation with the Committee, 3 October 2003.

14 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

15 Ms Liz Atkins, Australian Transaction Reports and Analysis Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

identity-related fraud in Australia.[16] This modelling study involved some 120 organisations in the public and private sectors including the financial industry, telecommunications and other infrastructure industries, and the retail industry. SIRCA's Report which was released in November 2003, is of great importance for the strategic planning of other public sector agencies in their response to identity fraud issues (Cuganesan & Lacey 2003). Although originally intended to improve the 100-point system used to identify people who open accounts with financial institutions, the Working Party has broadened its focus to address more general issues concerning identity fraud.

In a separate initiative in 2003, the Australian Government established a Steering Committee to examine common proof of identity processes used in public sector agencies. This committee, with representatives of federal as well as state and territory government agencies, is working to ensure that the most effective identification procedures are in place to achieve efficient service delivery while minimising the risk of fraud.[17]

As part of the investigation of proof of identity processes, the Australian Government has also commenced an investigation into the concept of an online verification system to enable data to be verified between agencies that issue primary documents used for establishing identity, such as birth certificates, drivers' licences, passports etc. The idea of an 'Electronic Gateway' is being investigated at present and, if implemented, could assist in the early detection of instances in which counterfeit or altered documents were submitted as evidence of identity for a range of purposes.

The Australian Government also has an E-Security Co-ordination Group (ESCG) which is chaired by the National Office for the Information Economy (NOIE). This includes representatives from agencies with an interest in defence, economics, revenue protection, regulatory and criminal law enforcement, telecommunications and broadcasting and industry development. It aims to realise the potential of information technology without prejudicing national interests.[18]

In May 2003 the New South Wales Parliamentary Library published a Briefing Paper on identity fraud and related matters that examined the nature and extent of the problem, and legislative and other responses from a New South Wales perspective (Lozusic 2003).

There are also some specific industry initiatives designed to address particular fraud problems. Project Angus, for example, is a Working Group involving major Australian banks and has been established to facilitate the creation of a framework in which secure electronic transactions can be carried out using the

16 Ibid.

17 Ibid.

18 Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

Identrus scheme (NOIE 2002). Similarly, a joint initiative of the University of Melbourne and the Australian Commercial Galleries Association aims to develop policies and procedures to deal with paintings of questionable authenticity in the Australian art market.[19]

Each of these initiatives, at federal, state and territory level, as well as those involving industry bodies and representatives, aims to deal with either general or specific issues that need to be resolved in order to minimise fraud risk in Australia. Victoria is involved in many activities already, but needs to prepare policy responses that will enhance and reinforce existing initiatives rather than duplicate or detract from them.

Purpose and limitations of this Report

The purpose of this Report is, then, to review current knowledge with respect to the issues raised by the Terms of Reference and to identify the most effective and appropriate options for reform that could be implemented in Victoria.

The Report draws upon and integrates existing sources of information on fraud and electronic risks including statistical studies, surveys, prior academic and business reviews, information from government agencies, legislation, published police and judicial materials, and various online sources. In order to confine the scope of the statistical data gathered and to ensure its greatest relevance to the discussion in Victoria at present, statistical data have generally been restricted to the period since 1960, with a major focus on the last five years. Generally, the Report focuses on current and emerging issues rather than being an historical review of the problems, although it is important to understand the way in which current problems have developed and changed over time.

This Report has not, however, involved the collection of new empirical or quantitative data (other than the integration of some official statistical sources). Rather, it makes use of current information that has, on occasions, been re-analysed in order to highlight trends applicable in Victoria.

In addition, this Report has drawn upon material received by the Committee in response to its public call for submissions, as well as material obtained in the public hearings conducted by the Committee in Melbourne and during its interstate visits, as outlined above.

19 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

Conclusion

As is apparent from the preceding discussion, this Inquiry raises issues of far-reaching import. The principal focus of this Report is on the problems of fraud and financial crime involving electronic commerce as they affect Victoria, although responses draw upon initiatives used elsewhere if they can be adopted effectively for use in Victoria. In addition, the Report examines the problems of fraud and electronic commerce and best practice solutions in the context of both public and private sector agencies. As can be seen in subsequent chapters, there is no single solution to fraud and white-collar crime.

In the words of Hon. Justice Frank Vincent

> When you ultimately come down to the notion of fraud, you are really talking about people taking from other people. The techniques can vary, but that is what it amounts to. Are you going to stop people from doing this? I doubt it. I am not sure that people have ever been entirely honest throughout history and I rather doubt that we will change that situation in our lifetime.[20]

This should not, however, deter policy-makers from seeking out appropriate and effective solutions, some of which may have existed for many years, and others of which are yet to be devised.

20 Hon. Justice Frank Vincent, Justice of the Supreme Court of Victoria, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 November 2003.

2. The Nature of Fraud in Victoria

Introduction

As indicated above, there are various ways in which to categorise fraud and white-collar crime. This chapter begins by considering why people commit acts of dishonesty, with particular reference to psychological profile. It then looks at fraud from the perspective of various occupational sectors that are regularly targeted by offenders, or within which offenders work. These include the public sector, the professional sector and the corporate and business sector. The chapter concludes with some examples of fraud against consumers, particularly focussing on the elderly. Dishonesty involving electronic commerce exists throughout these sectors, but will be examined in more detail in Chapter 4.

This chapter considers the nature of fraudulent activities committed by offenders who are located in Victoria or who target Victorian victims. The extent to which this occurs and issues associated with quantifying the problem will be discussed in Chapter 3.

Motivating factors

Duffield and Grabosky (2001) describe some of the key motivational and psychological factors that lead to the commission of offences of dishonesty. They argue that fraud, like other crime, can best be explained by three factors:

1. A supply of motivated offenders,
2. The availability of suitable targets, and
3. The absence of capable guardians.

As Nettler observes:

> [T]he intensity of desire and the perception of opportunity are personality variables. The balance between desire and opportunity moves. Temptation to steal fluctuates with individual temperament and situation (Nettler 1974, p.75).

Motivation is, therefore, a combination of an individual's personality and the situation in which they find themselves. Conversely, psychological factors will influence the way individuals interpret the situation they are in, and this in turn will influence the action they choose to take.

Just as the technologies used for legitimate electronic commerce may readily be adapted to criminal ends, the same is true at the psychological level. As Duffield and Grabosky note, '… some of the same qualities that facilitate fraud are also integral to successful commercial activity of a legitimate nature' (2001, p.5). Legitimate activity is not always easily distinguishable on the surface from its illegitimate or illegal counterpart.

Greed and organised crime

On occasions, however, fraud is committed by determined groups of organised individuals who are motivated solely by financial gain. A number of submissions received by the Committee noted an increase in recent years of organised criminals in fraudulent activity involving external attacks on banks, superannuation funds and business.[21] Evidence from a representative of the Corporate Crime Liaison Group, for example, stated that, 'we have seen… in the last couple of years… an increased involvement of organised crime in fraud, and I have seen comments from a lot of people talking about the shift away from drugs – drug importation and drug trafficking – to fraud'.[22]

The Committee also heard that there has been a recent shift in the focus of organised crime from drugs to fraud, and that there was an increased incidence of organised criminals from other countries (commonly from parts of Asia) operating in Australia with a proven *modus operandi* before returning to their country of origin. One example concerns international telephone call centres being targeted by organisations in order to acquire people's personal information.[23]

Organised crime is no longer confined to one type of activity and offenders are now beginning to experiment with multiple competencies such as drug trafficking, trading in weapons, people smuggling and financial crime (see Mackenzie 2002). In Queensland, for example, identity-related fraud has been

21 Mr Bruce Cox, Regional Director–Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003; Mr Ray Bange, Acting Manager, Misconduct Prevention Unit, Crime and Misconduct Commission, in conversation with the Committee, Brisbane, 26 June 2003; Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003; Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

22 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

23 Dr Clive Summerfield, Manager for Government Services, VeCommerce Ltd, in conversation with the Committee, Canberra, 24 June 2003.

found to be committed by organised crime groups.[24] In particular, credit card fraud is now often perpetrated by overseas-based international crime groups. In the words of Acting Detective Superintendent Peter Lavender of the Western Australia Police, Commercial Crime Division, 'there is clear evidence that credit card fraud and identity fraud in particular are becoming the focus of organised crime groups. These groups have identified that the benefits of these offences far exceed the associated risks'.[25]

Greed lies at the heart of much dishonest activity in the community, although not all those who are aggressively acquisitive break the law (Duffield & Grabosky 2001). Often the desire or perceived need to maintain an inappropriately extravagant lifestyle leads to the commission of fraud.

In the 1980s a number of individuals engaged in wide-ranging activities in which investors were defrauded of many millions of dollars (Brown 1998). Peter Badger, for example, used various managed investment schemes to defraud his clients of more than $700,000 over six years. In 1996 he was sentenced to six years imprisonment and was banned for life from working in the investment advisory industry. In dismissing his appeal, the Court of Criminal Appeal said:

> The sentence, whilst undoubtedly severe, was within the proper exercise of the sentencing discretion. The appellant was in a position of trust. His fraudulent conduct extended over a period of about six years. A very large sum of money was involved. Giving due weight to the appellant's undoubted remorse and his pleas of guilty, this clearly was a case where a penalty which was calculated to reflect the enormity of the appellant's criminal conduct and to have general deterrent effect was called for (R. v *Badger*, Court of Criminal Appeal, Supreme Court of Tasmania, 7 April 1997).

The largest investment fraud in Australia's history was perpetrated by an accountant, David Gibson, who defrauded 600 clients out of $43 million in the 1980s, again using managed investment funds and employing a Ponzi scheme[26] in which early investors were paid dividends out of the investments of subsequent investors. Gibson was sentenced to 12 years' imprisonment with a non-parole period of nine years (R. v *Gibson*, County Court of Victoria, 24 June 1993; see the discussion of this case in Brown 1998).

---

24 Mr Ray Bange, Acting Manager, Misconduct Prevention Unit, Crime and Misconduct Commission, in conversation with the Committee, Brisbane, 26 June 2003.

25 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Sydney, 1 October 2003.

26 Charles Ponzi – whose name has become synonymous with a certain type of fraudulent investment practice – established the 'Financial Exchange Company' in 1919 which guaranteed a 50% return to investors within 45 days. The company purported to buy international postage coupons in countries in which the exchange rate was low, and resell them in countries with higher rates. Within six months, 20,000 investors had provided nearly US$10 million. Unfortunately, the dividend paid to early investors came from the money invested by new investors. After an exposé in the *Boston Globe* on 2 August 1920, Ponzi was arrested and convicted of fraud (Rosoff, Pontell & Tillman 1998, p.5).

Maintaining a lifestyle

Often so-called 'lifestyle cases' arise because of changes in individuals' financial circumstances that are beyond their control. For example, solicitors have been subject to considerable pressures in recent years since the implementation of Competition Policy, which has resulted in the collapse of their monopoly over conveyancing. In 1995 the Industry Commission in Australia estimated that the introduction of competition reforms in the legal profession would result in a 50 per cent reduction in conveyancing costs due to the removal of the profession's monopoly over conveyancing work, and a 13 per cent reduction in barristers' fees through the removal of advertising restrictions (Tonking 1995). In fact, a comparison of conveyancing fees between 1994 and 1996 conducted by the Justice Research Centre found that the mean professional fees charged by small law firms decreased in real terms by approximately 17 per cent because of increased competition (Baker 1996).

This meant that some solicitors had to seek out new sources of income. Unfortunately some succumbed to the temptation to act illegally and to defraud their clients in order to maintain their existing standard of living. Corporate researcher, Mr Tim Farrelly, in his evidence to the Committee, noted that 'ego and lifestyle' were some of the main reasons for financial services fraud, particularly where individuals were unable to admit losses or were involved in maintaining appearances through possessions.[27]

Financial strain and problem gambling

Financial strain caused through excessive personal expenditure on goods and services was identified as a major cause of financial crime. The cost and addictive properties of illicit drugs may also contribute to financial stress on the part of those individuals who indulge in them, sometimes resulting in those affected stealing funds to finance their addiction. Relationship breakdowns can also cause acute stress, both financial and emotional, especially given expensive divorce settlements and custody/maintenance battles. In some cases marital breakdown can represent a sudden and dramatic decline in an individual's standard of living, along with a feeling of powerlessness and resentment. This constellation of factors reflects the old-time detectives' explanation of what turns a person to fraud – 'sex, substance abuse and risk taking/gambling' (Nettler 1982, p.74).

In these cases, the explanation may be taken into account as a mitigating circumstance, although the conduct will clearly be dishonest and culpable. Cases involving solicitors and accountants who misappropriate client funds in order to fund compulsive gambling activities or to purchase drugs of addiction occasionally come before the courts.

27 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

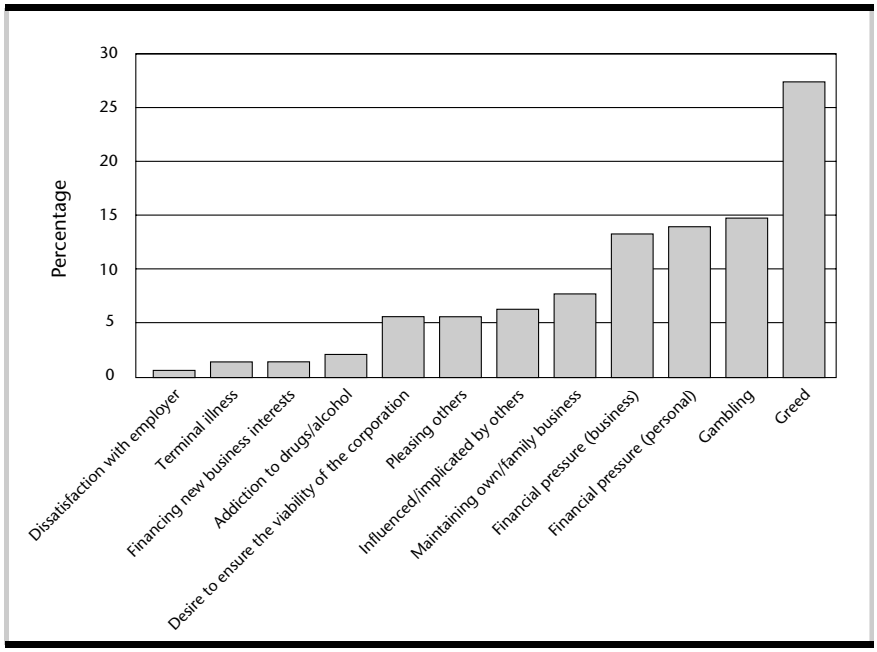
One area that has been examined in recent research concerns the relationship between problem gambling and the commission of financial crime (Sakurai & Smith 2003). It has been estimated that problem gamblers represent 2.1 per cent of the Australian adult population (1 per cent with severe problems and a further 1.1 per cent with moderate problems). Although the number of problem gamblers appears small, they contribute to approximately one-third of total expenditure on gambling in Australia. In addition, their annual losses average $12,220 compared with under $650 for other gamblers (see Sakurai & Smith 2003).

In one study conducted in New South Wales, Crofts (2002) examined 2,779 cases heard by Local and District Courts between 1995 and 1999. The study examined a variety of property offences involving fraud (eg. obtaining financial advantage by deception, making false statements with intent to obtain money or a financial advantage, or presenting cheques with insufficient funds), theft (eg. larceny, larceny by a clerk or servant, or stealing in or from a dwelling house, or motor vehicle theft), robbery and assault, and breach of apprehended violence orders. These types of offence were selected as representing those most likely to establish a link between gambling and crime. Files involving these offences were made available at the New South Wales District Court in Sydney for inspection by researchers and provided a cross-section of property and violent crimes against the person dealt with by Local and District Courts in the five years in question. Pre-sentence reports and police reports were examined to find evidence of gambling or gambling-related activities. An offence was classified as 'gambling-related' if it was: 'committed as a consequence of, or committed in order to support, or committed as a significant result of, or significantly related to the defendant's desire, need or compulsion to gamble' (Crofts, 2002, p.29).

Of the 2,779 cases examined by Crofts (2002), 105 cases (4%) were found to be gambling-related. Of these cases, 42 contained insufficient detail for further analysis, leaving 63 files that provided the basis for the final study. Of the 63 cases in the final sample, 76.2 per cent of offences committed involved fraud, including larceny by a clerk, obtaining financial advantage by false pretences, and cheque fraud. The 27 larceny by a clerk files that were gambling-related involved a total amount stolen of $2,494,309 and a mean amount stolen by each offender of $95,935.

Another study carried out by the Australian Institute of Criminology and PricewaterhouseCoopers examined a sample of 'serious fraud' prosecutions heard in 1998 and 1999 in Australia and New Zealand. The sample consisted of 155 separate files involving 208 accused persons, 183 of whom were convicted of charges. As is apparent from Figure 2.1, gambling (14.7%) was found to be the second most frequently identified motivation of convicted offenders after greed (27.3%).

Figure 2.1: Primary motivation of convicted serious fraud offenders



Note: Information on motivation was available in respect of 143 out of the 183 convicted offenders.
Source: Australian Institute of Criminology and PricewaterhouseCoopers 2003, *Serious Fraud in Australia and New Zealand*, Research and Public Policy Series No. 48, Australian Institute of Criminology, Canberra.

Of the 21 convicted offenders (in 20 files) whose primary motivation for fraud was gambling, the vast majority (86%) spent the proceeds of their crime on gambling itself (Sakurai & Smith 2003).

In one Victorian case heard on 13 March 2003, an accountant and former mayor of Geelong was sentenced to 10 years' imprisonment with a non-parole period of seven years after pleading guilty to defrauding his clients of $8.6 million between 1994 and 2000. He was known and trusted by many members of the Geelong community but abused that trust by stealing funds from a number of his clients. One count involved the sum of $4.98 million that had been stolen from a trust account established to administer an award of $6 million damages paid to the victim of medical negligence which had rendered him quadriplegic. After becoming one of the signatories to the bank account established to hold the client's funds, the offender made a number of unauthorised withdrawals that were used initially to replace sums stolen from other clients and subsequently for gambling. In all, the offender lost $7.1 million of the illegally obtained money through gambling. As a VIP member of a Casino, he spent 937 days there over seven years, managing to conceal his activities from his family and the community by sometimes linking business trips to Melbourne with visits to the Casino (R. v *De Stefano*, [2003] VSC 68, Supreme Court of Victoria, 13 March 2003).

In another Victorian case, a 44 year-old man who had been employed by an insurance company since he was 17 years old had been working as a senior claims officer between 1991 and 2000. He had been gambling for some time but lost control of his habit in 1991, to the extent that he found it necessary to mortgage his then unencumbered family home in the sum of $35,000 in order to cover credit card and gambling debts. The mortgage was increased the following year to $75,000. In order to obtain further funds to support his gambling, the offender re-opened completed claims, authorised them, and created 1,003 fraudulent cheque payments to a total value of $4,328,520 to fictitious third parties purporting to relate to the re-opened claims. The cheques obtained were paid into accounts opened in his own name with various banks, ostensibly as trustee for one or another of the fictitious third parties. Most of the money so obtained was lost through gambling. He was sentenced to seven years and six months imprisonment with a non-parole period of five years and six months (R. v *Atalla* [2002] VSCA 141, Supreme Court of Victoria, 27 August 2002).

More recently, a West Australian bank manager, Kim Faithfull, was convicted of stealing $18,998,309 from his employer, the Commonwealth Bank, between 1 April 1998 and 7 August 2003. He was sentenced to five years' imprisonment, with a three-year non-parole period (Pitsis 2003). The sentence is, however, subject to appeal by the Director of Public Prosecutions (Cowan & Eliot 2003). The fraudulently obtained funds were used in part for gambling on horse races.

These cases are supportive of comments made in a number of the submissions received by the Committee concerning the influence of problem gambling on the commission of fraud offences.[28] The evidence of a representative of the Corporate Crime Liaison Group, for example, noted that:

> [P]eople are going out at lunch time and they are spending their lunch time at a local pokie machine venue, coming back to the office having lost money, and seeing the solution to their financial dilemma sitting in front of them in terms of stealing from their employer. We have had many cases over the past couple of years where it has been four or five million stolen for gambling.[29]

Generally, funds are stolen to repay debts incurred through gambling, rather than to gamble in the first instance.

The Corporate Crime Liaison Group's representative continued: 'We think there is a need to address the issue of problem gambling because we do find that is a very common motivator for people who commit fraud, not just in Victoria but

28 Ms Leanne Joy Clare, Director of Public Prosecutions for Queensland, in conversation with the Committee, Brisbane, 26 June 2003; Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

29 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

also interstate and overseas'.[30] Independent researcher, Mr Tim Farrelly, noted that in approximately one-quarter of financial services frauds he had examined, financial advisers had sought to make good losses incurred through gambling.[31]

Power

Duffield and Grabosky (2001) also note the desire some people have for power over others as well as power over situations. In terms of the former, the sensation of power over another individual or individuals seems to be such a powerful motivating force for some fraud offenders that it becomes an end in itself. As one confidence man put it:

> 'For myself, I love to make people do what I want them to, I love command. I love to rule people. That's why I'm a con artist' (quoted in Blum 1972, p.46).

In manipulating and making fools of their victims, some fraud perpetrators seem to take a contemptuous delight in the act itself rather than simply the outcome.

Rationalisations

Duffield and Grabosky also refer to the process of rationalisation which reduces the offender's inhibition. These attempts by fraudsters to explain away and excuse their own unethical behaviour have been termed 'techniques of neutralisation' (Sykes & Matza 1957). There has been a tendency in the literature to confuse motivation with neutralisation, but they differ in important ways. Motivation is what drives the act of fraud, while neutralisation paves the way by nullifying internal moral objections. Regardless of the type of fraud, most offenders seem to seek to justify or rationalise their activity. In doing so they will use 'vocabularies of adjustment' (Cressey 1953, 1986) that manufacture a rationale or generate extenuating circumstances so as to remove their own perception of criminality from their actions. Neutralisation contributes to a lowering of the fraudster's moral inhibitions.

Techniques of neutralisation vary with the type of fraud (Benson 1985). For example, frauds against large companies or government departments are often rationalised with the excuse, 'They can afford it'. Other examples of neutralisation include viewing the victim as culpable in some respect, or trivialising the offence so that it comes to be seen as a 'victimless crime' or one in which no significant harm is done. Those frauds that involve a victim entering willingly and knowingly into an illegal act (such as money laundering or tax evasion) are among the easiest for the fraud offender to rationalise. In such cases it becomes easy to believe that the victim 'had it coming'. In his study of confidence men and their activities, Blum (1972) found that many attributed their success to the inherent greed of the victim. Many con artists also seemed

30 Ibid.

31 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

to have a misanthropic view of human nature and assumed that others were as scheming and dishonest as they were. There is no doubt that generating a dislike and lack of respect for the victim makes it easier to treat them badly.

Weak restraints

Stotland has proposed that as well as positive motivations for white-collar crimes such as fraud, there are also 'weak restraints' that lessen the inhibition about committing these crimes (Stotland 1977, p.191). One of these weak restraints is the perception that everyone engages in this behaviour as part of astute business or financial practice. In this way, practices such as tax fraud, insurance fraud and padding expense accounts become normal behaviour and those that don't participate are seen as naive. Stotland goes on to point out that the moral ambiguity surrounding some types of fraud is exacerbated by the characteristically short sentences meted out to offenders. In high profile cases, the leniency of punishment tends to weaken the criminal stigma attached to fraud in the eyes of the public. Stotland also states that the victimisation of 'impersonal' entities such as government departments and large organisations makes it morally easier to defraud. Stealing a little from a lot of people means that harm is not as 'up close and personal' as it would be in the case of an individual victim or small group. This is similar to the 'they can afford it' neutralisation mentioned earlier (Duffield & Grabosky 2001). The depersonalised, technologically mediated character of electronic commerce makes this a particular concern (see Chapter 4).

Misunderstandings

Finally, the least serious forms of dishonesty might be said to arise through poor communication resulting in consumers believing that they have been defrauded or deceived in some way when, in fact, a legitimate explanation exists. Examples might include solicitors failing to be clear in describing the circumstances in which costs are incurred or in which monies are debited from client accounts for legitimate purposes – although in some instances solicitors may deliberately fail to provide full details to their clients for dishonest reasons. A number of complaints arise each year in Victoria against solicitors for over-charging or misappropriation of funds that involve poor communication between practitioners and their clients (Neville 2000). In these cases criminality is generally not involved, although the practitioner may well be guilty of failing to adhere to proper professional standards of conduct.

Fraud in the public sector

Occasions have arisen in which public servants, often successfully, have sought to defraud government agencies both directly and indirectly. Direct theft may occur when employees steal petty cash or remove government property. More covert forms of theft involve the abuse of government facilities such as the unauthorised use of motor vehicles and computers. Government employees may abuse their position by accepting bribes to grant licences for which there is no entitlement or by charging governments for goods or services which are not actually provided (see Mills 1999).

The scale of such conduct varies from the trivial, for example having an extended lunch break, to the serious, such as large-scale misappropriation of funds from government departments. Little systematic research has, however, been undertaken into the nature and extent of the losses which governments have sustained. Although agencies record information on the extent of fraud for their own internal fraud control purposes, they rarely share it publicly. Many governments would prefer that their fraud experiences never be made public in order to avoid criticism for not having appropriate preventive measures in place. Brief summaries provided in annual reports or media reports of cases involving prominent figures are often the only references to this fraud that are publicly available.

Changes within the public sector have created new opportunities for fraud. To the extent that goods and services previously delivered by government institutions and public services have been contracted out to the private sector, opportunities for fraud from within the public sector have been reduced. However, a corresponding increase in opportunities for fraud by outside contractors, with or without the complicity of public servants, may be expected. In addition, there is the possibility that the process of contracting out services may itself create new opportunities for crime. Already this has resulted in millions of dollars being lost through collusive tendering and the granting of secret commissions to obtain contracts (Smith 2002b).

The largest Commonwealth agencies such as the Australian Taxation Office, Centrelink, and the Health Insurance Commission are regularly victimised through fraud, a proportion of it perpetrated by Victorians. One submission received by the Committee, however, considered that fraud was not a major problem in the public sector in Victoria, because most government funds were provided by Commonwealth agencies.[32] Nevertheless, some areas of concern have been identified in Victoria. Mr Wayne Cameron, Victorian Auditor-General, expressed the view that a number of irregularities had been identified in the State Revenue Office and that this Office had commenced action to prevent recurrence of these problems.[33]

32 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

33 Ibid.

Another area within the Victorian public sector that has shown increased levels of fraud in recent years is that involving higher education, particularly TAFE Institutes. Although relatively low numbers of incidents are reported officially, there have been a number of matters dealt with by the police in Victoria in recent years. A survey of fraud and fraud control within the TAFE sector was conducted by a consultant engaged by the office of Training and Tertiary Education. The survey found that less than 30 per cent of TAFE Institutes had a fraud control strategy; approximately 50 per cent had formal fraud reporting systems, and only 35 per cent of respondents had carried out a fraud risk assessment.[34] A submission to the Drugs and Crime Committee relating to fraud in one TAFE Institute made allegations of sales tax fraud and improper use of government facilities.[35]

In giving evidence to the Committee, a representative from the Victorian Auditor-General's Office noted that TAFE colleges have notified a number of cases of fraud and loss each year, most involving theft of equipment that has taken place either through burglaries or through equipment 'just going missing'. At one of the Committee's public hearings the comment was made that 'how much of that is employees misusing or taking equipment and how much is genuine theft or just losses is hard for even the TAFE colleges to identify at times'.[36]

In 1994 the Australian National Audit Office conducted an audit of a sample of transactions undertaken with the Australian Government Credit Card (Australian National Audit Office 1994). Since the card was introduced in November 1987 until March 1994, there were 46 cases of fraud reported totalling between A$1.8 million and A$2.0 million for all departments and agencies. The bulk of cases related to claims under A$5,000, as shown in Table 2.1.

34 Ibid.

35 Submission from Mr Geoff Griffiths to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 10 July 2002.

36 Mr David Reid, General Manager, Financial Audit, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

Table 2.1: Reported Australian government credit card fraud and misuse 1987–94

Value of Fraud	Incidence
> $1 m	1
$50,000 - $100,000	1
$10,000 - $20,000	5
$1,000 - $5,000	12
< $5,000	14
Value unreported	13
Total	46

Source: Australian National Audit Office 1994, *The Australian Government Credit Card: Some Aspects of its Use, Audit Report No. 1, 1993–94*, Project Audit, Australian Government Publishing Office, Canberra.

Most of the frauds related to the purchase of goods for unauthorised private purposes or for travel and hospitality, which had been paid for from other sources ('double dipping'). Of a sample of 1,866 card transactions examined, the Australian National Audit Office identified 523 instances of misuse of cards, some of which had not been formally reported. These instances included 336 transactions where the use of the card was not correctly approved, was outside guidelines for use, was inappropriately used or was questionable.

Dishonesty in connection with nursing homes is also an area of concern, although most instances relate to fraud against Commonwealth agencies. Such cases usually involve medical entrepreneurs and business people rather than health care providers such as doctors and nurses, although occasionally professionals may be involved. Arguably Australia's largest nursing home fraud involved a Sydney nursing home operator and pharmacist who was convicted of defrauding the Commonwealth in January 1997. The defendant had operated five nursing homes and had stolen $1.7 million in Australian government funding through lodging false claims for costs allegedly incurred in respect of the nursing and personal care of frail aged residents in the homes. Claims were made in respect of family members, non-existent employees on the nursing payroll and other staff not involved in nursing or personal care of residents, such as builders, bricklayers, and contractors (*Comfraud Bulletin* 1998, p.3).

Fraud in the professional sector

Fraud in the professional sector continues to be a major concern, largely because of the ever-increasing opportunities for dishonesty to occur in the professions (see Smith 2002a). In Australia in 2001 there were approximately 1.5 million professionals, according to the Australian Bureau of Statistics (2001). Professionals were the largest occupation group in Australia, making up 18.2 per cent of the total Australian labour force. There were also 975,653

associate professionals, making up an additional 11.8 per cent of the labour force. Together, professionals and associate professionals comprised 30 per cent of the nine million Australians aged 15 years and over in the employed labour force in 2001.

In Victoria in 2001 there were 399,158 professionals and 236,451 associate professionals, which together constituted about 30 per cent of the Victorian labour force, and just over 25 per cent of all professionals and associate professionals in Australia (Australian Bureau of Statistics 2001).

Professionals also now make extensive use of information technologies. In a 1998 survey conducted of Victorian legal practitioners, 2,684 responses were obtained out of 8,500 surveys distributed by the Law Institute of Victoria (Kriegler 1999). Sixty-three per cent of respondents were male, with the majority aged 30 to 49 years (57%). Forty-four per cent of respondents indicated that they had access to the Internet on their desks, 57 per cent had Internet access elsewhere in their office and 35 per cent had access at home. Forty-eight per cent of respondents used the Internet for legal research, 57 per cent for electronic mail and 37 per cent for Web browsing (Kriegler 1999).

Electronic communications technologies, such as the Internet, are also enabling consumers of professional services to be better informed about matters that previously lay within the province of professional advisers. Members of the public are now able to conduct their own share dealings online and obtain advice about legal matters. One of the largest English firms of solicitors now provides online information and advice about local laws, regulations and other details to global investment banks operating in Europe, the United Kingdom and Asia for a yearly fee of up to £125,000 for unlimited access to the service (Gray 1999).

Although fraud can occur in all professional groups, the following discussion will focus on the three professional groups that tend to show greater susceptibility to fraud problems: the legal, accountancy and health care professions.

Lawyers

In Victoria, approximately 2,300 complaints are made each year concerning the conduct of solicitors (Neville 2000). These relate to problems of delay, poor attitude, over-charging, and misappropriation of funds. Twenty-one practitioners were referred to the profession's tribunal for a disciplinary hearing in 1999. Of those cases, 12 had their practising certificates cancelled or reduced and were fined; seven were fined without restrictions being placed on the practising certificate; and two cases were dismissed. On average, six practices a year are taken over by the Law Institute in Victoria because of trust account defalcations, which represents approximately 2 per cent of the 3,411 solicitors authorised to handle trust funds in that state. Most cases related to misuse of

investment funds, although since controls have been placed on solicitors' mortgage practices these cases have reduced substantially (Neville 2000).

Cases involving trust account defalcations in Victoria have been described as being perpetrated for various reasons, additional to the desire to maintain a certain lifestyle. Some practitioners said that they were trying to assist a desperate client; others were attempting to cover errors with other clients' trust funds; in some cases trust funds were used to cover financial crises within a joint practice; or to keep a failing or poorly managed practice alive. In other cases the funds were used to finance gambling or other addictions. Invariably the practitioner is unable to repay the funds and the deficiency in the trust account becomes apparent (Neville 2000). Although clearly illegal and unethical, in such cases as these the reason behind the conduct is understandable as being due more to ineptitude or incompetence than to the more morally culpable motivation of personal greed.

Circumstances can also arise in professional practice in which a practitioner is drawn into criminal activity that is being conducted by a dishonest client, or advises a client concerning a proposed course of conduct that might be illegal (Williams 2002). Such conduct is sometimes hard to characterise as dishonest as it may involve the practitioner acting with undue zeal on behalf of a client and in the process lead to an unintended and unforeseen breach of professional ethical principles or criminal laws. For example, advising clients as to the circumstances in which it is legal to do certain activities, such as minimising taxation or destroying documents that could be relevant to legal proceedings, could sometimes lead to the professional adviser aiding and abetting a criminal act, or otherwise acting contrary to professional ethical standards (Cox & Wallace 2002).

Trust account misuse can also arise out of inadequate professional standards or poor levels of training, while other cases have involved inept investment of client funds or investment outside regulatory controls. In one Queensland case, a solicitor pleaded guilty to having misappropriated approximately $4 million from client trust account funds for investment in a Nigerian advance fee letter scam. He was sentenced on 5 May 2000 to 10 years imprisonment for one count of misappropriation and five years imprisonment concurrent for two counts of uttering false documents. It was ordered that he be eligible for release on parole after three years of that period (R. v *Crowley*, District Court of Queensland, 5 May 2000).

In the case of R. v *Fulton* (Supreme Court of Tasmania, 13 December 2001) a solicitor had used client trust funds amounting to $98,000 for the payment of settlement monies due to other clients which the practitioner failed to secure due to incompetent handing of civil litigation on their behalf. He was convicted and sentenced to two years and six months imprisonment, suspended after he had served 14 months.

Accountants

Those in the accounting profession have also been involved in acts of dishonesty. Sometimes this has involved overt acts, such as theft of client funds or theft of practice assets. On other occasions the dishonesty has been more difficult to characterise as criminal. This occurs where a practitioner is drawn into criminal activity that is being conducted by a dishonest client, or advises a client on how to act illegally.

Where, for example, an auditor discovers fraud within a client's company but fails to take action by reporting the matter to the police, it is sometimes unclear that the auditor has acted improperly. Recently the International Federation of Accountants has suggested amendments to International Standard of Auditing (ISA) 240, which will place a greater onus on auditors to make sure that fraud control measures are in place and to report suspicious financial transactions (Gettler 2000).

In Victoria, when announcing the revised Australian Auditing Standard AUS 210, the Chairman of the Auditing and Assurance Standards Board said that:

> The Standard is part of an ongoing international effort to increase auditors' ability to detect fraud … Whilst some elements of AUS 210 may be considered as onerous by some auditors, in times where corporate collapses have brought the efficacy and integrity of auditors under close scrutiny, it is difficult to objectively argue that greater attention should not be paid to fraud.[37]

Recent data collated by Aon Risk Services Australia Ltd, relating to its financial planners' indemnity insurance facility, indicate that claims involving 'misappropriation of funds' made up only 7 per cent of the number of reported claims, but 37 per cent of the dollar value of all claims made. If the value of claims attributed to quasi-dishonest behaviour such as 'conflict of interest' and 'misleading statements' are added, the total claims from this broad description of dishonesty rise to approximately 50 per cent of the dollar value of all claims made against financial planners (Williams 2002).

In addition, professionals in the financial services industry can also commit acts of dishonesty. In giving evidence to the Committee, Mr Tim Farrelly noted three main types of fraud that can take place in relation to the delivery of financial services – embezzlement (where financial advisers direct client funds to themselves rather than for investment purposes), placing client funds into fraudulent investments, and unauthorised trading or failure to reported losses incurred through trading, such as where trading takes place without the authority of the client, and the adviser engages in further trading to recoup losses.[38]

---

37 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002 citing the Chairman of the Auditing and Assurance Standards Board.

38 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

On occasions the consequences of professional misconduct in the financial services industry can be extensive, such as has been seen recently in the case of the collapse of Enron and WorldCom corporations. Where professional advisers have acted improperly, criminal proceedings can be taken, such as occurred in the case of Ben Glisan, the former Treasurer of Enron who was convicted of conspiracy to defraud investors of the corporation and sentenced to five years' imprisonment in the United States (Elliott 2003).

In Australia, the corporate collapses of HIH and One.Tel have not resulted in criminal convictions, although the former Chief Financial Officer of Harris Scarfe Limited, Alan Hodgson, was sentenced to an effective term of six years' imprisonment with a non-parole period of three years. The case related to his actions in falsifying the accounts of the major retailing chain over a prolonged period of time. From 1994 until 2001 Hodgson was in charge of the finance and accounting staff of Harris Scarfe Limited and oversaw the production of all the financial and accounting records of the Harris Scarfe group of companies, including the group's consolidated accounts. It was alleged that Hodgson directed staff under his control to make false entries in the books of account, which had the effect of showing an inflated level of profits. Reports showing these misleading profit figures went to the board of the Harris Scarfe group of companies and the Australian Stock Exchange. It was not clear when the practice began but it continued until Hodgson left Harris Scarfe Limited in March 2001. It required an extensive financial analysis by officers of the Australian Securities and Investments Commission (ASIC) to unravel the financial accounts (Commonwealth Director of Public Prosecutions 2002).

Health care providers

Electronic funds transfer systems are quickly becoming the principal means by which payments are made to and from health care providers. This has created opportunities for electronic claim forms to be counterfeited, digital signatures to be manipulated, and electronic funds transfers to be altered or diverted from their legitimate recipients.

Attempts to profit illegally from medical claims systems are regularly reported by the Health Insurance Commission (HIC) which has a statutory mandate to prevent, detect and investigate the fraud and abuse of government health programs, including the Pharmaceutical Benefits Scheme (PBS) and Medicare. A recent case prosecuted by the HIC involved a psychiatrist who was alleged to have made claims amounting to more than $1 million in respect of false referrals received from more than 100 general practitioners over approximately a six-year period. The referrals were never made by general practitioners but were fabricated by the psychiatrist through forging signatures and creating false referrals and benefit assignment forms (see Cauchi 1999).

In 2001, a number of Victorian pharmacists were prosecuted for their involvement in over $1.3 million of fraudulent PBS claims uncovered by a joint investigation by the HIC and the Australian Federal Police's 'Operation Denver'

(Health Insurance Commission 2001b). One Melbourne pharmacist was found to have defrauded the HIC of $1.1 million in pharmaceutical benefits over a two-and-a-half year period to help finance her struggling business. She was convicted and sentenced to 18 months' imprisonment, wholly suspended (R. v *Thi Thuy Nguyen*, County Court of Victoria, 13 June 2001). Her accomplice, who obtained $350,000 from the scheme, was sentenced to three years' imprisonment with a non-parole period of two years (R. v *Phuong Thi Le*, County Court of Victoria, 5 September 2002).

Dishonesty can also arise out of a conflict of interest between professional advisers and their clients. There have been cases in which doctors have prescribed drugs or medical appliances for improper motives. These motives include having a financial interest in the company selling the drug or appliance, or receiving an inducement from the company. One recent manifestation of a much older problem has arisen where medical practitioners have used the World Wide Web to advertise their professional activities or provide information to the public, but are in breach of the ethical standards of acceptable practice. In one case a famous doctor in the United States maintained a web site that contained material advertising particular health products. It was alleged, however, that he had failed to disclose a commercial interest in the products being advertised and sold through the web site (see Noble 1999).

Sometimes professional advisers will become privy to information that could be used for their personal advantage and then make use of that information dishonestly. This may infringe client confidentiality or involve a misuse of confidential information. An example of a case of 'medical insider trading' was the so-called 'MRI scam' uncovered in late 1999, in which up to 300 Australian radiologists were allegedly involved. The HIC has reported that the radiologists backdated orders for MRI machines, or used revocable contracts, in order to profit illegally from a 1998 budget decision to introduce Medicare rebates in respect of scans carried out on privately owned machines. The rebates were applicable only for machines purchased or ordered prior to the date of the budget announcement. Some 33 machines were ordered six days before the announcement, with 27 of these allegedly made on the basis of inside knowledge of the proposal (Zinn 2000). The HIC sought repayment of $164,000 from one doctor in respect of payments made for MRI scans that had been requested by a general practitioner rather than a specialist, as required by the HIC (Gray 2000; see also Australian National Audit Office 2000a).

Medical practitioners have also been involved in accepting fees from drug companies to carry out controlled trials of new drugs but then failing to conduct the trials and instead simply submitting fabricated results.

Sometimes practitioners use their clients' funds for speculative investment purposes, such as the case of a doctor in New South Wales who misappropriated patients' money intended for an investment scheme and was later convicted and deregistered (New South Wales Medical Board 1993). On

other occasions practitioners may be experiencing personal financial difficulties and misappropriate client funds to invest in order to maintain their income.

The other area in which dishonesty has arisen concerns practitioners who have exerted undue influence over their clients to leave them bequests in their wills or have sought to borrow money from clients, which they are unwilling or unable to repay.

Dishonesty can also arise in non-financial circumstances. For example, health care providers have sometimes misrepresented the nature of treatment provided for inappropriate personal reasons. In a widely publicised case, a medical practitioner diagnosed as HIV positive, engaged in unprotected sexual intercourse with his partner over an extended period without disclosing his medical condition. He was charged and pleaded guilty to one count of recklessly engaging in conduct which placed a person in danger of serious injury, one count of obtaining financial advantage by deception and one count of attempting to obtain financial advantage by deception. He was sentenced to four years and two months' imprisonment with a non-parole period of three years. On 25 August 1997 his name was removed from the Medical Register by order of the Medical Practitioners Board of Victoria. The Board's Panel found him guilty of:

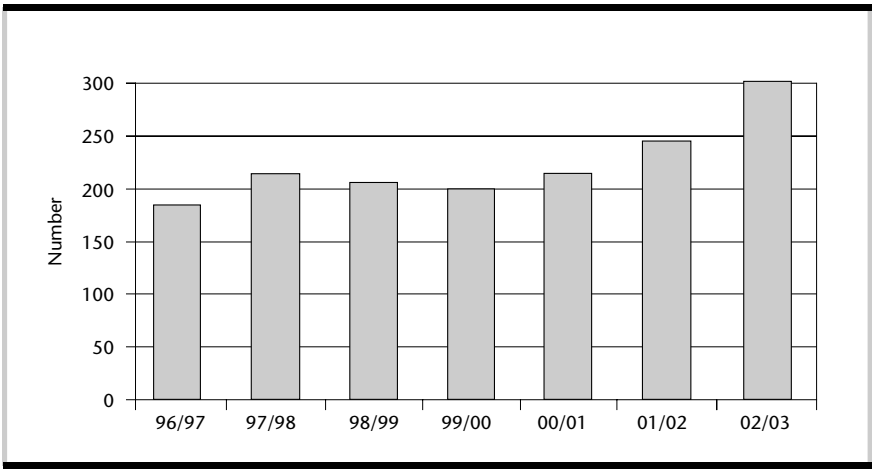
> … abuse of trust by having unprotected sexual intercourse with two current patients, by flagrantly defrauding Medicare, by misusing the doctor/patient relationship to borrow large sums of money from existing patients, and by encouraging an untrained person known by him to be HIV positive to assist in minor surgical and office procedures (R. v *Dirckze* County Court of Victoria, 13 August 1999 *per* Anderson J).

It also found that he had compounded these grave abuses of trust by knowingly exposing one patient to the risk of transmission of HIV by engaging in unprotected anal sexual intercourse with the patient (R. v *Dirckze* County Court of Victoria, 13 August 1999).

Fraud in the corporate and business sector

In Australia, the Corporations Law is administered and enforced by ASIC. ASIC investigates instances of non-compliance with the Corporations Law as well as consumer protection laws concerning investments, life and general insurance, superannuation, and banking (excluding lending), and it prosecutes those found in breach of the law. Victorian offenders are included in cases prosecuted by ASIC each year. Data for investigations commenced between 1996/97 and 2002/03 are presented in Figure 2.2.

Figure 2.2: ASIC investigations commenced, 1996/7–2002/3



Source: Australian Securities and Investments Commission 1997 to 2003, *Annual Reports 1996-97 to 2002-03,* Australian Securities and Investments Commission, Sydney.

Large-scale frauds committed by company directors misappropriating shareholders' funds continue to be a problem. These can occur by various means, from the payment of loans or 'management fees' to the director's family company, to the purchase or sale of goods and services between the public company and the director's family company on terms extraordinarily favourable to the latter.

Cases of insider trading and market manipulation are also regularly investigated by ASIC, while fraud and misrepresentation with respect to fundraising activities occurs in relation to corporations as well as securities markets (Smith 2002b).

Ina recent case, stockbroker Rene Rivkin was sentenced to imprisonment for a term of nine months, to be served by way of Periodic Detention, with a fine of $30,000 for insider trading as defined in section 1002G of the *Corporations Act 2001*. Mr Rivkin was found to have purchased 50,000 shares in Qantas shortly after hearing of a potential merger between Qantas and Impulse Airlines (R. v *Rivkin* [2003] NSWSC 447, Supreme Court of New South Wales, 29 May 2003; Australian Associated Press 2003a).

Insurance

Insurance fraud can take a variety of forms. These vary from limited exaggeration of the value of a claim, to an entirely bogus claim where losses never really occur. In the past this was an increasing problem, although the efforts taken by the insurance industry have been very successful in reducing the incidence of fraudulent claims. For example, in 1991 the Insurance Council of Australia (ICA) estimated that approximately $1.7 billion was paid out in respect of claims arising out of fraud and arson in Australia, but in 1994 this was reduced to approximately $500 million (Insurance Council of Australia 1994).

However, a representative of the ICA claims that fraud still adds an extra $21 to the cost of every general insurance policy issued in Australia.[39] The ICA estimates that for each dollar paid by an insurance company in relation to an arson claim, a further $8 of public money is expended for the maintenance of services such as the police, fire brigades and the courts, as well as to cover the dislocation of services where, for example, employees of a factory destroyed by arson are forced out of work and on to social security payments.

Financial services

Although not often discussed in public by corporations reluctant to acknowledge the nature and extent of their victimisation, fraud committed against financial institutions is an area of ongoing concern. It is also an area likely to grow in importance as electronic banking continues to develop. Clearly not every incident of fraud can be investigated by financial institutions, as the costs associated with investigating some low-value incidents may outweigh any likely return. Nonetheless, financial institutions have much at stake and on occasions have suffered substantial losses. Some of the key areas of fraud were identified recently by Chapman and Smith (2001).

Mr Aub Chapman also noted in conversation with the Committee that as technologies such as EFTPOS, ATMs, Internet and online banking, and Bpay continue to develop, opportunities for financial crime are facilitated.[40] Information provided to the Committee from American Express identified its three largest emerging fraud risk areas as being identity fraud, counterfeit credit cards and mail-order fraud. Mail-order fraud occurs when, for example, a credit cardholder uses the card to purchase goods or services, such as a restaurant meal, following which an employee of the merchant records the card numbers, expiry date and authentication code and makes use of that information to order goods by telephone from a retailer.[41] In the view of one submission to the Committee, card-not-present fraud, especially committed over the Internet, was seen as a major inhibitor to the growth of electronic commerce in Australia.[42]

In its submission to the Committee, a representative of Victoria Police noted that the main types of fraud in Victoria are identity-related fraud and credit card-related fraud.[43] Evidence to the Committee from Victoria Police also noted that law enforcement had seen an exponential growth in credit card fraud through card cloning and skimming, mirroring trends overseas. Victoria Police

39 Information provided by Mr Peter Eagle, Insurance Council of Australia, to the Fraud Advisory Council of the Institute of Chartered Accountants in Australia, 14 April 1998.

40 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, In conversation with the Committee, Sydney, 25 June 2003.

41 Mr Bruce Cox, Director, Global Security, American Express, and Mr Jilluck Wong, Regional Director- Fraud Prevention, American Express, in conversation with the Committee, Sydney, 25 June 2003.

42 Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

43 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

also stated that International criminal groups were actively committing a variety of fraudulent activity, in particular credit card and identity-related crimes, within Australia. Identity-related crimes are evident in most fraud-related offences including loan applications, credit card fraud and online banking. Identity-related crimes were noted to be currently one of law enforcement's greatest problems globally, although significant efforts to combat this criminal methodology were now being addressed by a number of forums nationally.[44]

Cheque fraud

While it is necessary to try to predict the fraud risks associated with the future direction of business practices, it is also important to recognise that the more traditional financial services products remain a major area of vulnerability to fraud. Negotiation of valueless cheques, stolen cheques, forged cheques, altered cheques, and counterfeit cheques remains fertile ground for those seeking to commit fraud. In a number of instances these activities are well-organised and involve a number of parties. Theft of cheques from the postal system, the use of scanners, colour photocopies, and chemicals to alter existing documents or even to create entirely false documents, demonstrate a trend away from single opportunists to more deliberate, wide-spread attacks on the financial services industry (Chapman & Smith 2001).

Plastic card fraud

The introduction of plastic credit and debit cards as a means of payment in an ever-expanding marketplace has been accompanied by forms of fraud. Lost and stolen cards, lost/misused Personal Identification Numbers (PINs) and the practices of corrupt card merchants have all provided new channels through which to conduct attacks on financial institutions. Turnover in the workforce of financial institutions, coupled with the growing amounts of information available on the Internet, have added greatly to community knowledge of financial systems and the inherent weaknesses in some products and services. For example, individuals have defrauded financial institutions by exploiting ATMs which operate 'off-host' (unconnected in real-time to financial institutions' computer networks, eg. *Kennison* v *Daire* (1986) 160 CLR 537; R. v *Evenett* [1987] 2 Qd R 753, and R. v *Baxter* [1988] 1 Qd R 537). Thus, the provision of a service that enabled customers to withdraw cash at any time of the day and night led to the creation of a new fraud risk. Every innovation that enables payment or access to funds has vulnerabilities which are soon revealed

44 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

and exploited by fraudsters. Similarly, technology designed for use within the industry enabled the 'skimming' of account and personal information contained in the magnetic stripe on the back of the credit card, thereby facilitating the creation of duplicate and counterfeit cards. Card 'skimming' is a growing area of fraud that can cause significant losses to be suffered by some businesses (see Chapter 4).

Funds transfer fraud

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

The imperative to compete in a rapidly changing market has placed considerable strains on financial institutions to limit time-consuming validation and verification checks. Electronic commerce, for example, demands that transactions be executed instantaneously and that payment be provided immediately. This pressure has presented new opportunities for those seeking to benefit through fraud at the transactional level (Chapman & Smith 2001 and see discussion in Chapter 4).

Identity-related fraud

Over recent years the problem of identity-related fraud has taken on considerable importance, again facilitated by computing technologies (see Smith 1999; also 'Risks for individuals – Identity-related fraud' in Chapter 4 of this Report). Mobility within the community means that businesses no longer rely on local knowledge of an individual's background and circumstances when entering into commercial relations. A customer/business relationship is now usually commenced by the prospective customer presenting documents by which his or her identity can be verified. Through the theft and alteration of documents it is possible for one person to assume the identity of another, and where reasonable similarity is present (eg. same gender, similar age, etc.) it is not difficult to undertake business dealings in the other person's name. Alternatively, sometimes completely fictitious identities are created supported by entirely false documents. Credit facilities can then be provided or other benefits obtained, and the individual is unable to be located following default under contractual arrangements.

It is this initial stage in which the parties have had no previous contact that is most susceptible to abuse (Willox & Regan 2002, p.2). Where documentary evidence is the only means available to establish an asserted identity, the use of good quality, cheap technology facilitates identity-related fraud by enabling the creation of false documents. After the verification process has failed once, and a genuine document has been issued under false pretences, it becomes rather easy for a person to use that genuine proof of identity document to procure other documents and so build a new, illegitimate identity.

The results of a pilot validation study conducted by the New South Wales Registry of Births, Deaths and Marriages and Westpac were that 13 per cent of birth certificates presented when opening new accounts did not match the records of the issuing agency. A second pilot study conducted by financial services organisations in Victoria, VicRoads and the Victorian Office of Births, Deaths and Marriages found that 18 per cent of birth certificates presented did not match the records of the issuing authority (Cuganesan & Lacey 2003, p.2).

An example of identity-related crime occurred in Victoria between August 1995 and March 1996. In the case of R. v *Zehir* (Court of Appeal, Supreme Court of Victoria, 1 December 1998), the offender used desk-top publishing equipment to create 41 birth certificates, 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. The accounts were used to pay cheques into as wages and make immediate withdrawals from before they had cleared, to register a business name, to obtain sales tax refunds, and to defraud various retailers. The offender was convicted of a variety of offences and sentenced to five years' imprisonment with a non-parole period of three years. He was also ordered to pay compensation of A$41,300 and reparation to the Commonwealth of Australia in the sum of A$458,383.

Cases of this kind were mentioned in a number of submissions to the Committee. At the federal level, an Australian Taxation Office representative noted that many deliberate attempts to defraud the taxation system are based around the misappropriation of identities.[45] In the private sector, identity-related fraud was seen to lie at the heart of most instances of fraud perpetrated in recent years.[46] Finally, identity fraud and theft was seen as one of the greatest problems facing law enforcement agencies in recent years.[47] Evidence

45 Mr Chris Barlow, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, Canberra, 24 June 2003.

46 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, Sydney, 25 June 2003; Mr Bruce Cox, Regional Director–Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003.

47 Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

from the Acting Detective Superintendent of the Western Australian Commercial Crime Division, for example, noted a vast new interest in identification theft and fraud in the recent past, although it was observed that there has 'just about always been an element of false identification involved in the offence of fraud'.[48] The existence of organised crime in identity and credit card fraud was also noted. The Committee heard that identity fraud and identity take-overs are increasing at a prolific rate with organised crime groups continually targeting document-issuing agencies and using professional printing businesses to print high quality fraudulent documentation in bulk.[49] The Acting Superintendent of the Commercial Crime Division also said that 'identity fraud is the means by which money laundering and terrorism are now facilitated'.[50]

Victoria Police also noted the importance of identity-related fraud:

> Identity crime has been clearly identified as an emerging challenge for Victoria Police. Presently in Australia, identity crime, which encompasses the use of fraudulent identities and identity theft, is growing at a rapid rate. The Australian Institute of Criminology has estimated that fraud in Australia now costs up to $5.88 billion per annum. Identity fraud is a large component of fraud. Much of the growth in identity fraud can be attributed to the advances in technology that facilitates the production of high quality fraudulent documents, or bypassing verification systems used in the public sector and government agencies. Intelligence suggests that Australian and overseas-based crime syndicates commonly perpetrate identity crime. Intelligence indicates that these syndicates are equipped with cutting edge computer software and other resources that assist them in the commission of these offences.[51]

Loan and investment fraud

The principal types of financial services fraud investigated by the police in Victoria include false valuation frauds, in which money is lent on the basis of inflated property prices; investment frauds, in which monies invested by agents are stolen; and false loan frauds, in which funds are borrowed using fictitious identities and then not repaid or the financial standing of loan applicants is fraudulently enhanced to enable loans to be taken out that are not repaid (Smith 2002b).

One recent example was the case of R. v *Jenkins* ([2000] VSC 503 Supreme Court of Victoria, 20 November 2000), in which the offender obtained loans and a guarantee from a lending institution in Victoria for the sum of $165

48 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

49 Ibid.

50 Ibid.

51 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

million over some 15 months from 4 May 1988 to 21 August 1989. The offender was found guilty of five counts of furnishing false information and five counts of obtaining a financial advantage by deception involving false representations in valuation reports of properties he had purchased and on the security of which he sought, and obtained, the loans. The offender was sentenced to seven years' imprisonment with a non-parole period of three-and-a-half years. In sentencing, Mr Justice Coldrey referred to the fact that the offender had been assisted in plundering the funds of the lending institution by the conduct of a dishonest and voracious mortgage broker, a dishonest and compliant valuer, and persons in positions of responsibility at the lending institution whose negligence and commercial recklessness ill-served the members of the organisation.

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

The offender fraudulently obtained nine birth certificates, two drivers' licences, three Medicare cards, one Christmas Club account book and eight bank passbooks and used them to obtain credit cards. There were 61 applications made of which 45 were granted. The offender made these by assuming the identity of a large number of persons, some of them fictitious but many of them real, and some of them known to her from her school days. The accounts were manipulated so as to obtain credit much in excess of the declared limit. These frauds, which involved about 12 transactions a week over a period of nine months, benefited the offender to the value of about $10,000 a month. While this was going on she was living in subsidised public housing, receiving between $250 and $300 a week from the Commonwealth by way of pension, child endowment and 'Austudy' and earning about $400 a week as a prostitute.

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

The committal for trial had been on 102 charges, compressed into a presentment containing 12 counts of obtaining property by deception. On 19 November 1998 there was a plea of guilty to the first nine counts, the last three having been deleted by arrangement. Each offence carried a maximum penalty

of 10 years' imprisonment. On the following day she was convicted and sentenced to 12 months' imprisonment on each count and cumulation orders were made of three months in respect of counts two to nine so as to give a total effective sentence of three years, with a non-parole period of two years.

The three-year sentence became the subject of an application for leave to appeal. Mr Justice Brooking observed that the offender systematically engaged in credit card fraud to obtain large amounts of cash and many and varied goods and services, and her claim to a psychologist that she personally obtained little benefit and was concerned only to keep her household running and to clothe her infant son was unreliable. The sophistication of the offences, the 'catastrophic effects of the frauds on some of those whose names were used' and the 'entire absence of remorse' exhibited by the offender were remarked on. At a more general level, Mr Justice Brooking also observed:

> the credit card has achieved ever-increasing popularity. For good or ill, it has for many people largely replaced cash as a means of payment. It has itself become an important source of cash advances. This case shows how someone can systematically abuse the system by fraudulently obtaining a stock of these plastic cards which stand in the place of money, and shows some of the injurious consequences of that abuse. Generally speaking, the kind of conduct disclosed here must attract severe punishment (R. v *Harrower* [1999] VSCA 182, Court of Appeal, Supreme Court of Victoria, 9 November 1999).

The sentence was not found to be manifestly excessive and the application for leave to appeal failed.

Small and medium-sized business

Small and medium-sized businesses are also at risk of victimisation through fraud, not only from customers but also from the staff they employ. It should also be noted, as one submission to the Committee emphasised, that merchants rather than financial institutions take the financial impact of fraud relating to electronic commerce, such as dishonesty involving card-not-present transactions conducted over the Internet, because such transactions entered into without authority are 'charged-back' to merchants.[52]

The following are some of the main categories of fraud experienced by small and medium-sized businesses in Victoria.

52 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

Refund fraud

One area of concern identified to the Committee was refund fraud.[53] Refund fraud occurs when customers abuse the lenient refund policies adopted by retailers to increase customer satisfaction (Freauf 1996, p.65). There are numerous ways in which refunds can be obtained dishonestly. First, refunds under false conditions may occur when a refund is claimed at a different shop from that at which the item was bought. This category includes full price refunds requested for discounted stock, unwanted gifts or stolen goods (Challinger 1996).

Secondly, so-called ticket switching occurs when the offender alters the price tag of an item to show a lesser price than was originally attached to the goods. The item is purchased for the lower amount and later returned for a refund of the original full price (Freauf 1996).

Thirdly, fraud-related shoplifting involves offenders stealing an item during or after the purchase of another item of the same description. The proof of purchase slip from the sale is used to gain a refund for one of the items (Challinger 1996). Other offenders use proof of purchase receipts discarded by paying customers (Challinger 1996). In other cases, the offender takes an item off the shelves and directly presents it for refund (Sennewald & Christman 1992).

Fourthly, gift voucher fraud occurs when retail vouchers are forged, misused or presented for cash refunds. Retailers often use gift vouchers as a substitute for cash in refund claims where the customer does not have any proof of purchase. This provides an opportunity for fraud, as the offender may duplicate the voucher or use it to obtain items illegally (Challinger 1996).

Refund fraud may also be committed or facilitated by staff within businesses. False refund fraud may occur when a staff member processes a non-existent refund and retains the refunded amount. The offender uses either proof of purchase documents from a previous sale, provides fictitious customer details in place of a receipt, or processes a refund without including a receipt (Challinger 1996).

Fraud through the voiding of sales transactions occurs when an employee uses the 'void' function of a cash register dishonestly. The intended purpose of the void function is to amend cashier mistakes or to grant instant refunds to customers who change their minds, by deducting the sums in question from the total day's takings. Fraud occurs when the employee voids a transaction after it has been completed and paid for, and then retains the money tendered by the

53 Submission (name withheld) received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002; Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

customer (Hume 1996). Because the transaction has been removed from the cash register record, the inconsistency does not appear in the accounts. This type of fraud is quick, easy and does not require refund policies to be followed.

Finally, refund fraud may involve employees colluding with outsiders, such as when an acquaintance of a staff member dishonestly obtains a refund from that employee (Bamfield 1998). Refunded goods may be stolen, bought from another shop, or there may be no goods at all. Some employees provide a refund for a greater amount than the actual price of the item.

In giving evidence to the Committee, Consultant Criminologist Mr Dennis Challinger provided the following examples of ways in which refund fraud can be perpetrated. Offenders may purchase a small item at the start of the day from a store in order to obtain the code that relates to that day's trading. They will then go to their car and generate receipts for high value goods, such as televisions, using a portable laptop computer and printer. They then return to the store, select a television, and take it to the counter with their manufactured receipt to claim a refund. Offenders have also been known to make bar codes at home with computer equipment and place them over the real ones, leading to the item being scanned at a lower price. They then tear off the new bar code, and return it for full price. Offenders may see it as preferable to steal something from a store and return it for a 100 per cent refund than sell it elsewhere for perhaps only 30 per cent of the value. Finally, Mr Dennis Challinger noted that refunds, as a percentage of total sales, amounted to between 8 and 10 per cent, possibly even higher in department stores. This was seen as providing a significant potential for fraud.[54]

False invoicing

False invoicing is a common strategy used to defraud businesses and is often successful owing to the absence of effective accounting procedures and internal controls. Insiders or outsiders may perpetrate this strategy against a business.[55] In one example of internal false invoicing, an employee on leave falsely invoiced his employer for $60,000 in respect of computer services which were never ordered or provided (Newlan 2000). A recent example of external fraud involved false invoices being sent to businesses in respect of the renewal of Internet web site addresses (.au Domain Administration 2001).

False invoicing often occurs when a business is sent an invoice for products that have not been received or may not even have been ordered. Alternatively, a legitimate invoice may be falsified by including other unordered items, or by

54 Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

55 During an informal briefing, Mr Andrew Tuohy from KPMG Forensic advised the Committee on the various ways in which false invoicing can occur (Informal meeting with Mr Andrew Tuohy, Senior Manager, KPMG Forensic, Melbourne, 30 August 2002).

increasing the price or changing the identity of the vendor (Criminal Justice Commission, Queensland 1993). Another common strategy involves selling advertising space in an obscure magazine. A business will receive a telephone call 'confirming an agreement'. The call may relate to amendments to previously ordered advertising or may claim that another employee has agreed to place the advertising in question. In fact, the business never formally requested the advertising at all (Leamy 1997). The victim business is then faxed a page-proof of the advertisement, which is usually photocopied from a business directory. Finally, an invoice is sent and unless the terms of the agreement are verified and authorised, payment may be made, with little chance of recovery once the fraud has been discovered.

The extent of fraud in this category is not to be underestimated. A survey in Victoria of medium and large-sized businesses conducted in 1994 found that false invoicing alone was estimated to cost $21.7 million per year. Those most heavily affected by false invoicing were the transport, retail, and manufacturing industries. Of the 447 respondents to this survey, 50 reported instances of false invoicing carried out by internal and external offenders. It was found that the number of instances of fraud perpetrated by employees in middle management was equal to the number of instances committed by external suppliers (Deakin University 1994).

Telemarketing fraud

Small and medium-sized businesses are also at considerable risk of telemarketing fraud (Harrington, cited in Gips 1998). Its most direct impact on businesses occurs when a persuasive telemarketer contacts a business and persuades the manager to purchase business supplies, sometimes with the aid of attractive incentives. When an arrangement has been agreed to, the business is requested to pay for the products up-front, only to find that the goods are either not delivered or are of sub-standard quality (Grabosky & Smith 1998).

This kind of fraud is also perpetrated against individual consumers, with indirect consequences for businesses that may be no less damaging than direct victimisation. These scams increase suspicion of honest businesses and charities attempting to engage legitimately with customers through telemarketing, which may thus decrease their revenue (Grabosky & Smith 1998, p.138).

The extent of telemarketing fraud is difficult to quantify, mainly because victims often feel they are responsible and have contributed to their own victimisation. They may also feel foolish and thus be reluctant to publicise this fact.

Abuse of credit facilities

Abuse of lines of credit provided by suppliers of goods or services to small businesses can occur in a variety of ways. In its simplest form, a fraudster establishes a line of credit with the victim business, undertaking legitimate transactions in order to establish a degree of trust. The fraudster then orders goods (often involving substantial sums), defaults on payment and disappears (Churchill 1997).

Various strategies have been employed to obtain credit and to disguise the identity of the defaulting individual or company. The motivations behind such fraud also vary. Some may be established with the intention of engaging in fraud from the outset, while sometimes a legitimate business will resort to fraud due to desperate times (Levi 1981).

The former variety, sometimes known as 'long-firm fraud' operations, may have a high degree of specialisation, with a different person assigned for every task. Two positions common in such operations are 'front-men' and 'minders'. Front-men (who are occasionally female) are responsible for the day-to-day management of the business. The real business owner is concealed, and is therefore less likely to be pursued by authorities. 'Minders' communicate between the real manager and the front-man, visiting the business regularly to issue instructions and ensure there is no internal fraud (Levi 1981).

In the Deakin University study of fraud in Victoria, abuse of credit facilities was indicated to be less common than fraud entailing false invoicing. Nevertheless, this type of fraud was estimated to have cost Victorian businesses $165.9 million in 1994, which is significantly more than losses sustained through false invoicing. The primary perpetrators of credit-related fraud were customers of the business, closely followed by non-managerial employees within the business. The main industries affected by this type of fraud were found to be finance, transport and retail, respectively (Deakin University 1994).

A related type of fraud entails business managers who continue to trade on credit in the knowledge that they are unable to pay their debts as they fall due.

A survey in 1996 by the Australian Securities Commission (ASC) (as it then was) of small to medium-sized enterprises found that 36 per cent had sustained losses as a result of insolvent trading by suppliers' fraud. Insolvent trading may be facilitated by the Australian business community displaying empathy for businesses in financial trouble and by a reluctance on the part of creditors to take legal action to reclaim their assets in such circumstances. The results of the study indicated that 82 per cent of respondents would provide credit to an insolvent business, despite 59 per cent of all respondents disapproving of insolvent trading.

Another strategy employed to obtain credit dishonestly is the use of so-called 'phoenix companies', which deliberately avoid paying their outstanding debts, place themselves into liquidation, and conceal assets from liquidators. Shortly

after being wound up, the same directors, employees and assets reappear in a new company under a different name (ASC 1996).

Although problematic when they do occur, activities of this kind are much less common than insolvent trading. Only 18 per cent of respondents to the ASC survey were aware of having been victims of phoenix companies (Australian Securities Commission 1996). However, phoenix companies have been estimated to cost Australian businesses between $670 million and $1,300 million per year (Australian Securities Commission 1996). It is interesting to note that nearly half of those businesses affected (45%) were in the building and construction industry. The problem of phoenix companies in Victoria was investigated several years ago and various law reform solutions were proposed (Parliament of Victoria, Law Reform Committee 1995). Improved regulatory activity by the Australian Securities and Investments Commission has, in part, helped to minimise the problem of phoenix companies in Australia.

Art fraud

One final area of fraud that is of some concern for Victoria concerns the production and sale of counterfeit art works. Forgery can have a significant impact on the art market. It causes investors to lose confidence and when publicised can depress the sale of the particular artist or school that is subject to the forgeries. If international markets were to lose confidence in the authenticity of Aboriginal artwork, for instance, this could be particularly disastrous, as the art market is the source of many Aboriginal communities' economic livelihood.

The art industry, a subset of the luxury goods industry, is also attractive to money launderers because of the dearth of controls in the industry, the high value of quality art, and difficulties associated with determining the true value of art unless an experienced valuer is used. There is also an active market for quality art and no cash reporting requirements. Illicit funds can therefore be used to buy an item of considerable value without questions being raised as to the source of the funds (James 2000).

In the last few years Victoria Police has investigated a number of matters involving the authenticity of art works. They stated that 'only a small number of these matters are reported to police for reasons such as avoiding the embarrassment of the buyer who has spent large amounts of money'.[56]

56 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

Fraud against consumers

Individuals can also become the victims of fraudulent practices, particularly in relation to investment schemes and other misleading and deceptive marketing practices. Details of the many types of consumer-related frauds, particularly those involving electronic commerce, are set out in Grabosky, Smith and Dempsey (2001). Individual consumers also suffer the consequences of fraud committed against businesses through increased prices that are needed to compensate for losses sustained.

Advance fee scams

One area of concern identified in a submission to the Committee is the so-called 'advance fee letter scams', particularly those emanating from West Africa.[57] The gist of these is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some modest payment in advance.

The frauds discovered to date have taken a variety of forms. All have entailed victims being approached by letter or electronic mail without prior contact. Victims' addresses are obtained from telephone and email directories, business journals, magazines or newspapers and letters are invariably handwritten, often with counterfeit postage stamps being used, resulting in their being seized by postal authorities. They generally describe the need to move funds out of Nigeria and seek the assistance of the victim in providing bank account details in an overseas country and administration fees needed to facilitate the transaction. The victim is offered a commission, which could be up to 40 per cent of the capital involved. Capital sums of between US$20 to $40 million are often mentioned thus creating a potential reward for the victim of up to US$16 million. An advance payment that could total up to US$50,000 is usually required, which represents the amount stolen. The mechanics of the schemes extend from the barely plausible to the unlikely, but all have met with varying degrees of success.

The United States Secret Service estimated that between 1989 and 1999, US$5 billion was stolen from victims throughout the world, including Australia. Between August and November 1998, in Sydney alone, Australia Post confiscated 4.5 tonnes of advance fee correspondence which had counterfeit postage, amounting to approximately 1.8 million items. Early in July 1998, Australian Customs intercepted a courier package sent from Nigeria which contained 302 advance fee letters which were to be posted in Australia to destinations in New Zealand, the Pacific Islands and the South East Asian region. In March 1998, Hong Kong police arrested 54 persons and seized 13,350 advance fee letters (Smith, Holmes & Kaufmann 1999).

57 Ibid.

One individual in Victoria was reported to have lost $400,000 through such a scam involving advance fee letters sent from West Africa.[58]

There is a wide range of dishonest practices directed at individuals and these are regularly documented in surveys of consumer fraud victimisation (see 'Electronic crime and eFraud surveys – Consumer eFraud surveys', Chapter 3). Unfortunately, most of the evidence comes from the United States and there are few surveys conducted specifically in Australia or in Victoria of consumer fraud victimisation. Some indications of victimisation in relation to Internet transactions are presented below in the discussion of electronic commerce fraud risks (Chapter 4).

The following sections look at the fraud issues associated with two sectors of the community which, for different reasons, may suffer from a higher than average degree of vulnerability to fraud – the elderly and young people.

Older persons

One documented area of specific concern relates to dishonest practices perpetrated against older people in the community. A stereotype that surrounds older people is that they are easy targets for acts of fraud and deception. This stems from a perception that they have declining mental abilities and a dependence on others due to their physical fragility or mental deterioration. They are also seen as being isolated, often having few friends or family on whom they can rely, which makes them vulnerable to those who seek to establish relationships for the sole purpose of stealing their money (Smith 2000).

As with most stereotypes, this view of older people has some basis in reality, and some older people are indeed victimised through fraud. Generally, however, the extent to which older persons are defrauded is directly proportional to how vulnerable they are made by the circumstances in which they live. Old age of itself does not predispose someone to being deceived and defrauded any more than does gender or nationality. In fact the experiences of a lifetime may make older persons more able than younger people to detect a fraudulent proposal when it is made and avoid its consequences (Smith 2000).

In recent years, research into so-called 'elder abuse' has identified financial abuse of older persons as one of a range of forms of victimisation to which older persons may be subjected (Kinnear & Graycar 1999). Financial abuse includes making improper use of an older person's property or money without his or her knowledge or permission, forcing older persons to change their wills to benefit specific individuals such as health care providers or relatives, and denying older persons access to their money or preventing them from controlling their assets (Kurrle, Sadler & Cameron 1992).

58 Ibid.

Older persons, like others in the community, may be victimised through fraud when they purchase goods and services and the nature and extent of their victimisation will depend upon the nature of the goods and services they obtain.

Because older people spend a larger proportion of their time on domestic activities and recreational pursuits than on income-producing activities (Australian Bureau of Statistics 1999), it is to be expected that they may be vulnerable to fraud carried out by those who sell home maintenance and leisure products and services. As many older people spend considerable time at their homes, they rely to a large extent on information provided by broadcasting and telecommunications services, and may be vulnerable to frauds perpetrated using these media.

Older persons, and sometimes their relatives, may also be victimised through the purchase of pre-paid burial and funeral services. Sometimes the deception might never be discovered, as relatives of the deceased might not be aware that a pre-paid arrangement had been entered into. In Victoria, a company that made improper use of funds people had provided for pre-paid funerals was convicted in July 1999 of failure to invest the money in accordance with legislative requirements of the Office of Fair Trading and was fined $25,000 (Farrant 1999).

A wide variety of misleading and deceptive practices occur in the automobile repair industry (some of the fraud charges available in this area appear under 'Transport-related offences' in Appendix C-2). They include the carrying out of unnecessary repairs, overcharging, deceptive advertising, and the use of accelerated maintenance schedules. Older persons may be defrauded by such practices in the same way as others, although their unfamiliarity with some of the most recent technological advances in automobile design may make them particularly susceptible to fraud.

Telemarketing fraud, discussed in relation to businesses earlier in this chapter, has been a considerable problem for older persons for many years. Some studies have found that older people are more often defrauded through telemarketing scams than are younger people. In 1995, for example, the American Association of Retired Persons conducted interviews with 745 victims of telemarketing fraud and found that older people were more likely to be victimised than younger people. Fifty-six per cent of the victims were aged 50 years or more, while this age group comprised only 36 per cent of the general population (American Association of Retired Persons 1996).

Another area of increasing vulnerability relates to the risk of fraud arising out of gambling, prizes and lotteries. These are often examples of advance fee schemes in which victims are required to provide funds in order to receive some benefit.

Related to lottery fraud are instances in which victims may be persuaded to donate funds to so-called charitable organisations that are illegitimate and non-existent. In such cases a victim who has not verified the authenticity of the

organisation with a body such as the National Charities Information Bureau may never realise that he or she has been defrauded and so may never seek official redress.

Older persons may also rely heavily on professional advisers such as lawyers, accountants, and investment advisers when dealing with retirement funds, some of whom may act unprofessionally. In one case investigated by the Victoria Police Major Fraud Group in 1996, a husband and wife aged 85 and 80 provided a sole practitioner solicitor with $200,000 to be invested on the basis of security by way of registered second mortgage. The solicitor then misappropriated the funds for his own use. The case is one of a number dealt with by police each year in which solicitors misuse client funds.

In one submission to the Committee it was argued that:

> … with an ageing society, having an emphasis on self-reliance for superannuation and retirement income, the potential for significant increases in superannuation fraud and false investment scams is a distinct reality.[59]

Similarly, evidence to the Committee from Detective Senior Sergeant Peter Wilkins of Victoria Police was to the effect that because there is an increased awareness that everyone has to provide for their own retirement, there is a heavier reliance on people to look after their own superannuation. As a result, there is a large amount of money being invested in superannuation funds, which creates an opportunity for fraudsters to misappropriate the funds and thus to dramatically affect people's health, wealth and retirement.[60]

Younger persons

Electronic commerce also raises concerns for the younger demographic of the population, both as potential victims and as offenders. Young consumers are recognised as an important segment of the economy, with their own distinct set of problems and needs. As the *Consumer Issues and Youth* report noted:

> Young Australians represent a $4 billion a year commercial market, but most observers believe that among youth there is a general lack of awareness of basic consumer rights and how to find and access available consumer services (Commonwealth Consumer Affairs Advisory Council 2002, p.6).

Although consumers of any age must take care whenever they enter into contracts, younger persons could be at greater risk if they are specifically targeted by those who advertise electronic products dishonestly. The previous Minister for Consumer Affairs in Victoria drew attention to this problem, advising young consumers to 'get into the habit of reading the fine print when

59 Ibid.

60 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

signing a contract and know where to turn for help before they wind up in debt'. Credit cards and mobile telephone bills affecting Victorians between 18 and 25 years of age were highlighted in her remarks (Consumer Affairs Victoria 2001a).

There is potential for younger Internet users not only to be victimised but also to perpetrate frauds in various ways. Electronic commerce provides opportunities for young consumers who do not have access to credit facilities in their own right to make use of credit cards belonging to their parents or older family members without permission. Though more innocuous than other forms of credit card misuse, it should be recognised that the ability of minors to engage in financial transactions on behalf of their unwitting parents is now much greater than it has ever been. The relatively high level of Internet usage among young persons highlights this area as one that warrants further attention.

Finally, electronic commerce provides many opportunities for young people to engage in acts of identity deception. In 1987, for example, a group of schoolboys in Perth were apprehended after manufacturing cards and obtaining PINs by observing cardholders through binoculars (Tyree 1990, p.264). How to handle offences committed by precocious minors is one of the challenges faced in the electronic era.

Conclusion

The ways in which people can act dishonestly are only limited by one's imagination. History provides countless examples of people using ingenious means to steal property or to obtain benefits fraudulently. There are, however, numerous common motivational and personality factors that arise in crimes of deceit. Understanding the reasons why people act dishonestly provides a starting point for devising appropriate fraud prevention measures. In addition, being aware of the nature of the types of dishonest practices that have been employed in the past will enable many potential victims to avoid suffering similar types of losses at the hands of offenders in the future.

Having examined the range of fraudulent activities that have occurred in Victoria, the scale and cost of fraud will be considered in the following chapter.

3. The Extent of Fraud in Victoria

Introduction

There are many impediments to the accurate measurement of white-collar crime and fraud. Part of the problem lies in the absence of agreed definitions, which has prevented data from being collected in a uniform and consistent way. In Victoria, police statistics record 137 separate offences included in the category 'deception' and 170 other offences that have some relevance to fraud and dishonesty (see Appendices C–1 and C–2). These relate only to offences recorded by police, some of which may entail many individual counts of deception. In addition, and most importantly, these statistics only reflect matters coming to the attention of the police (see below). One submission to the Committee suggested that, in the writer's experience, 'fraud and white-collar crime in Victoria are far more prevalent than is indicated by official Victoria Police crime statistics'.[61]

A number of those who gave evidence to the Committee noted the general perception that fraud and computer-related crime are increasing. Victoria Police, for example, believed that the incidence of fraud and eCrime are on the rise, facilitated by advances in computer technology.[62] Acting Detective Superintendent Peter Lavender from the Commercial Crime Division of Western Australia Police Service also noted that 'white collar or corporate frauds have steadily increased at an alarming rate. One statistic that illustrates this increase is that the cost of fraud nationally is three times the cost of funding every State and Territory Police Service.'[63] The best that the Committee can hope to achieve in terms of quantifying the extent of the problem is to examine the incidence of crimes reported officially and matters reported in a number of fraud victimisation surveys. This chapter reports the currently available information on the extent of the problem in Victoria, and makes some recommendations as to how the data collection process could be improved.

---

61 Submission (name withheld) received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

62 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

63 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

Undetected, unreported and other 'not proceeded with' offences

Fraud tends to be a category of crime that often goes undetected, unreported or not proceeded with by law enforcement agencies.[64] This creates great difficulties for those seeking to obtain an accurate picture of the extent of the problem. Some victims, such as those who have given money to fraudulent and non-existent charities, may never realise that they have been victimised. Others, such as businesses, may be unaware that employees have stolen stock. In the case of fraud relating to electronic commerce, victims may be unable to locate the offender who may be resident overseas or who may have used an anonymous re-mailing system in carrying out the fraud.

Often the victims of economic crime may be unwilling to incur further time and expense in pursuing legal remedies and so respond by what is known in the dispute resolution literature as 'exiting' a problematic situation (Hirschman 1970). By refraining from taking legal action both the potential benefits to victims and the benefit to the wider community of deterrence will be lost. The offender is free to repeat the conduct at the same or another place of employment, and no external sign has been given to the rest of the community that white-collar crime is unacceptable.

There are many reasons why individuals and organisations may be reluctant to report frauds. In its most recent survey of business fraud, KPMG found that 62.6 per cent of frauds reported in the survey were referred to the police. This leaves nearly 40 per cent of fraud matters handled without police involvement. A range of other responses was reported, including internal and external investigations, or simply immediate dismissal of the individual in question (KPMG 2002).

Respondents to Deakin University's (1994) survey of fraud incidents against businesses in Victoria gave several reasons for not reporting fraud to the police. These included a belief that the matter was not serious enough to warrant police attention, fears of a consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter.

Similar reasons for non-reporting of electronic commerce incidents were given by the respondents to KPMG's *Global eFraud Survey* (2001), in addition to the key factor of the need to re-instate systems quickly so as to prevent loss of business. Reporting the matter to the authorities simply prevented the organisation in question from minimising its financial losses, and risked incurring further losses in prosecuting the matter.

Businesses are reluctant to report fraud simply due to a fear of 'sending good money after bad'. Their experiences may have led them to believe that it is impossible to recover losses through legal avenues and that the time and

64 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

resources required to report an incident officially and to assist in its prosecution simply do not justify the likely return on investment. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The other disincentive to taking official action lies in the reluctance of organisations to publicise their victimisation because of a fear of losing business or damaging their commercial reputation. A government agency that is the victim may believe that adverse publicity could result in a loss of confidence by voters, while financial institutions that have suffered from fraud might believe that publicity of security weaknesses could result in being targeted again.

A number of these factors were also evident in the results of the Australian Institute of Criminology's (AIC) survey of small businesses which included some crimes involving fraud. Drawing on data from the Small Business Crime Survey, it was found that crime reporting behaviour of small retail businesses varied, depending on the type of crime and whether the crime was attempted or completed. While nine in 10 completed burglaries and robberies were reported to police, only one in 17 incidents of employee theft, one in five incidents of shoplifting, and one in four incidents of cheque/credit card fraud were reported. Reasons for non-reporting generally reflected a pessimistic belief that reporting crime was pointless and achieved nothing (see Taylor 2002 and discussion below). Chapter 8 discusses some ways in which the under-reporting of fraud can be addressed.

The problem of under-reporting fraud offences was emphasised by a number of individuals with whom the Committee spoke. Mr Andrew Tuohy, for example, observed that while KPMG's *Fraud Survey 2002* found that 50 per cent of companies had been subject to recent fraud, his experience was that:

> Most companies have had fraud within a recent period, the level of which is different depending on the industry and the control processes that take place… It does affect most companies, and it does affect most employees, because they will see some sort of fraud or theft occurring.[65]

Mr Tuohy also noted that only about 60 per cent of the *largest* frauds were reported to police:

> …which indicates…that companies are not reporting a significant amount of their fraud. If 40 per cent of their largest single frauds were not reported, then the percentage reported would obviously go down and be a lot less as the frauds got smaller.[66]

65 Mr Andrew Tuohy, Senior Manager, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

66 Ibid.

Similarly, Mr Dean Newlan, representing the Corporate Crime Liaison Group (as it then was), noted that fraud is on the increase, and that 'fraud is less likely to be reported to the police now than it was… 50 years ago, so if you applied the same reporting rates you would probably find the incidence of fraud is a good deal higher than is shown in those figures'.[67]

Under-reporting in the financial services sector was seen as being a particular problem. The main concern, as Commissioner Mal Hyde stated, is that reporting is often not in the commercial interests of banks.[68] In his evidence to the Committee Mr Paul Coghlan referred to a recent case in which a bank had provided 60 to 70 loans based on false information. Only four of these, however, resulted in default by the borrower and it was only these cases that the banks pursued.[69] From a prevention and intelligence perspective each of the 60 or so cases would have been relevant.

Mr Bruce Cox indicated that less than 5 per cent of American Express' total fraud incidents were reported, which was felt to be a similar proportion for most financial institutions. The decision to report was based on likelihood of arrest and it was submitted that if all fraud were reported, law enforcement officers would be unable to handle the huge volume of cases.[70] Acting Detective Superintendent Peter Lavender also remarked on this problem of under-reporting:

> I believe that there is a dark figure of fraud that exists that we don't know about. Because corporate bodies decide that there is a threshold, a nominated threshold, under which they won't report and over which they will bring it to our attention. That deprives us of a lot of intelligence as to exactly how much fraud there is. With electronic fraud at the moment, ID fraud, it is usually high volume, low cost fraud, which would mean that a vast area of fraud won't get reported to us and we would be left without knowing exactly what was going on.[71]

67 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

68 Commissioner Mr Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

69 Mr Paul Coghlan QC, Director of Public Prosecutions, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

70 Mr Bruce Cox, Regional Director, Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003.

71 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

Finally, the problem of under-reporting was also seen to exist in the public sector, with a representative of the New South Wales Audit Office observing that 'agencies just don't like to admit that they have a problem'.[72]

Official statistical sources of information

The nature and limitations of official statistics

Despite these limitations, a starting point in documenting the extent of the problem of fraud in Victoria is to examine official statistical information published by criminal justice agencies and other regulatory agencies.

Official statistics are gathered by police services, the courts and correctional agencies. Each of these organisations has different purposes in gathering statistics and different policies in making them available. Privately administered prisons, for example, may be reluctant to disclose data that are perceived as being commercially sensitive. It is also necessary to distinguish data collected purely for statistical purposes from data collected for intelligence and operational purposes. In some databases it is possible to make use of operational data for statistical trend analysis and research purposes.

Official statistics are also collected by the civil courts. These may be of great value in fraud cases in which civil actions have been taken concurrently or following criminal investigations, particularly in describing the circumstances of the offences and losses sustained.

Official statistics, however, have their limitations. The first problem, despite the best efforts of those involved, relates to their accuracy. The English economist, Sir Josiah Stamp, in his 1929 book *Some Economic Factors in Modern Life*, described this problem as follows:

> The government are very keen on amassing statistics. They collect them, add them, raise them to the *n*th power, take the cube root, and prepare wonderful diagrams. But you must never forget that every one of these figures comes in the first instance from the village watchman, who just puts down what he damn pleases (Stamp 1929, pp.158–9).

The greatest possible care is needed not only in gathering data but also in determining which data are to be gathered. 'Village watchmen' need to be provided with clear, unequivocal guidelines in collecting data and entering information in computerised databases. Because official police statistics record only incidents reported to the police they give little indication of the true extent to which crime occurs in the community. If taken at face value they can be very misleading. Any changes in police detection rates, for example, or other factors that increase crime reporting and detection can affect the number of incidents that appear as official statistics.

72 Mr Tom Jambrich, Assistant Auditor-General, NSW Audit Office, in conversation with the Committee, Sydney, 25 June 2003.

Commonwealth matters involving Victorians

Each year, a number of cases of fraud committed against or by Victorians are investigated by Commonwealth agencies. Unfortunately, since official statistics are often presented in aggregate form, it is frequently impossible to determine which matters concern Victorians.

An indication of the size of the problem of fraud dealt with by the Australian Federal Police is set out in Table 3.1 which shows the number of economic crime cases referred for investigation between 1997 and 2003.

Table 3.1: Australian Federal Police number and value of economic crime cases referred for investigation, 1997–2003

Case type	1997-98	1998-99	1999-2000	1999-2000	2000-2001	2001-2002	2002-2003
Fraud							
Number	360	308	312	311	265	193	208
$000	125,970	104,410	207,269	212,696	148,954	267,541	–
Corporate, bankruptcy, intellectual property							
Number	83	87	53	56	56	36	46
$000	4,807	7,756	14,298	14,298	25,210	3,669	–
Computer/telecommunications							
Number	163	250	69	64	183	110	111
$000	229	3,215	1,101	1,101	49	100	–
Money laundering and FTRA							
Number	384	275	410	410	495	516	401
$000	101,578	70,751	60,358	59,553	135,858	180,612	–
Counterfeiting currency							
Number	180	146	95	90	95	51	27
$000	13,446	903	2,373	2,400	2,225	6,136	–
Environmental							
Number	5	2	4	4	7	14	17
$000	_	–	_	–	–	–	–
E–commerce							
Number	–	–	–	–	2	–	–
$000	–	–	–	–	5,000	–	–
Transnational economic							
Number	47	2,884	–	–	–	3	4
$000	40,837	–	–	–	–	–	–
Total							
Number	**1,222**	**1,069**	**943**	**935**	**1103**	**923**	**814**
$000	**286,868**	**187,012**	**285,399**	**290,048**		**458,058**	**–**

Source: Australian Federal Police 1997–2003, *Annual Reports*, Australian Federal Police, Canberra. (Value information is unavailable for 2002-03)

Some indication of the extent to which white-collar crime has affected Australian Public Service (APS) agencies in recent times may be gleaned from an examination of the results of an audit undertaken in June 2000 by the Australian National Audit Office (ANAO) on the fraud control arrangements in the Commonwealth public service (2000b). Of the 150 Commonwealth agencies surveyed, 106 responded to a question about the extent of fraud

experienced in the two years preceding the survey. Details of the extent of fraud reported are set out in Table 3.2.

Table 3.2: Extent of fraud reported by surveyed Australian public service agencies

	No. of fraud allegations		No. of fraud cases		Value of fraud cases ($ '000)	
	1997-98	1998-99	1997-98	1998-99	1997-98	1998-99
Internal	1,310	1,220	352	348	1,039	9,289
External	5,775	5,257	3,510	3,702	152,137	136,573
Total	7,085	6,477	3,862	4,050	153,176	145,862

Source: Australian National Audit Office 2002b, *Survey of Fraud Control Arrangements in APS Agencies*, p.29.

Some 40 per cent of these 106 agencies reported that they had experienced some fraud in the preceding two years, while more than 8 per cent of the frauds reported were committed against fewer than 10 per cent of the agencies. Although the greatest proportion related to external fraud – that is, by people not employed by the Commonwealth – these may still have been perpetrated by white-collar offenders. A number of problems were, however, encountered by the ANAO in measuring the extent of fraud in its survey. Seventeen per cent of agencies did not respond to the survey, two agencies were only able to provide data for 1998–99, and one agency only provided information on external fraud. Ninety-nine agencies provided data on the value of fraud, but six were unable to provide all the relevant data. Finally, agencies differed in their definitions of fraud, making comparisons difficult.

Victoria Police statistics

In Victoria, statistics are published on offences recorded by police, usually indicating the number of offences of particular types. However, definitions of offences have changed, new offences have been created and the categories used in compiling statistics have altered considerably. This creates serious difficulties in understanding how the level of officially recorded fraud has changed over time.

In the late 1970s an attempt was made by the Australian Bureau of Statistics to develop uniform offence categories. In 1985, the Australian National Classification of Offences (ANCO) category for offences relevant to the current inquiry was 'fraud and misappropriation'. Computer-related offences were not afforded a separate category. Then in 1987 a new national system was devised, the Australian Standard Offences Classification (ASOC), which now uses the category of 'deception and related offences'.

Prior to these standard categorisations, official police statistics relating to deception and fraud were grouped in a range of categories. These included:

- 'fraud, forgery and false pretences' (early 1970s);

- 'obtain by deception including offences against trust and currency' (late 1970s);
- 'fraud etc.' (early 1980s);
- 'fraudulent offences' (late 1980s); and since then
- 'deception offences'.

Separate categories were also used for court statistics and corrections statistics, although since the creation of the national system the ASOC category of 'deception and related offences' has tended to be used by all criminal justice agencies.

With respect to court statistics, deception and fraud matters recorded by the courts have used the following categories:

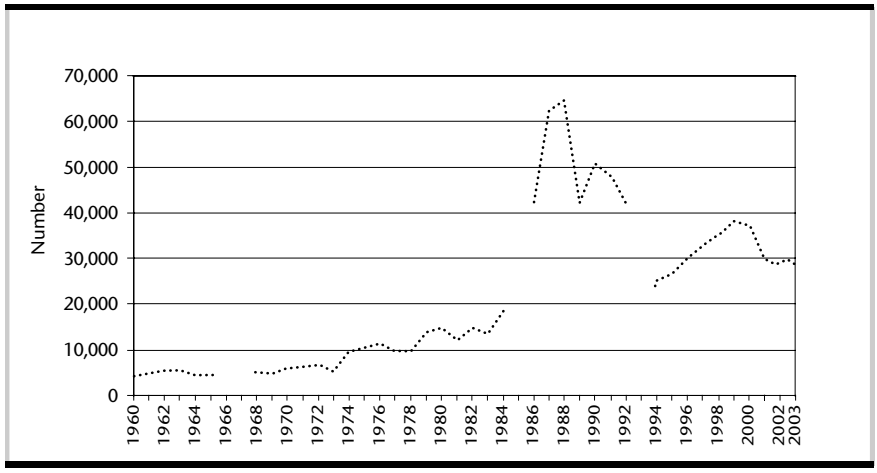
- offences of forgery and offences against currency only (Magistrates' Courts) (1960–1961);
- offences of embezzlement, false pretences, and fraudulent conversion (Higher Courts – County Court and Supreme Court) (1960–1962);
- offences of fraud, forgery and false pretences (Magistrates' Courts and Higher Courts – County Court and Supreme Court) (1963–1977).

In 1978, the categorisation changed from fraud, forgery and false pretences (1963–77) to fraud and deception, and following 1978 the draft ANCO categorisation was used. These changes resulted in an increase in the number of convictions recorded (for example, Higher Courts in 1978 – from 82 to 115 convictions). In 1979, Supreme Court statistics did not have a separate category for fraud and deception. After 1979, *Yearbook* court statistics only used the category 'breaking and entering, fraud, and other theft'.

In Victoria since 1 March 1993, Victoria Police has maintained a computerised database of offences, known as the Law Enforcement Assistance Program (LEAP). Data are recorded on each offence type and aggregated data can be extracted for major offence categories. Appendix C–1 of this Report sets out offences and major offence categories relating to fraud and deception currently used, and Appendix C–2 lists further miscellaneous offences relevant to this Inquiry.

Bearing these differences in offence categorisation in mind, it is possible to obtain a *general impression only* of how the number of officially recorded offences of fraud and deception has changed over the years. In the following charts the general term 'fraud' will be used, although the detailed offence category descriptions have altered over time. The detailed categories and data are set out in Appendix D. Principal trends in recorded fraud offences in Victoria between 1960 and 2003 are shown in Figure 3.1 below. Breaks in the charts indicate years in which statistics were unavailable or in which major changes occurred in the categorisation of offences.

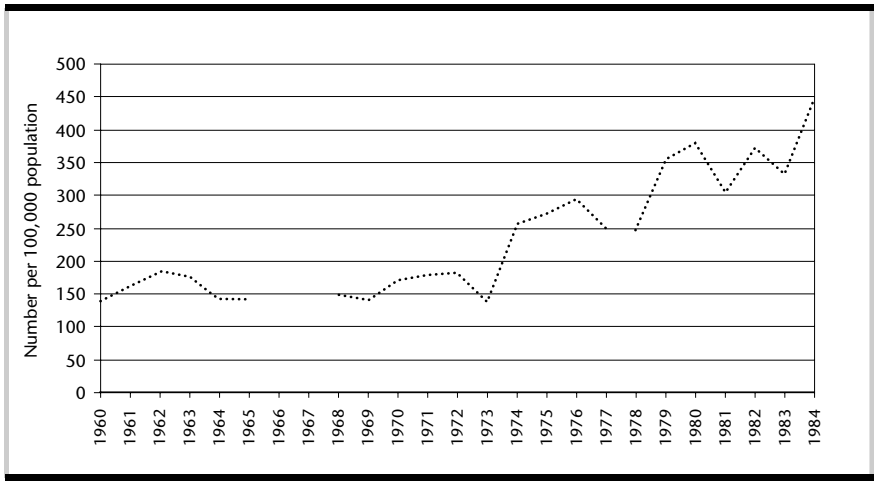
Figure 3.1: Number of Victorian fraud offences recorded by Police, 1960–2003



Source: See notes to Appendix D for sources, raw data and definitions of offence categories used. Breaks indicate years in which statistics were unavailable or years in which counting rules changed.

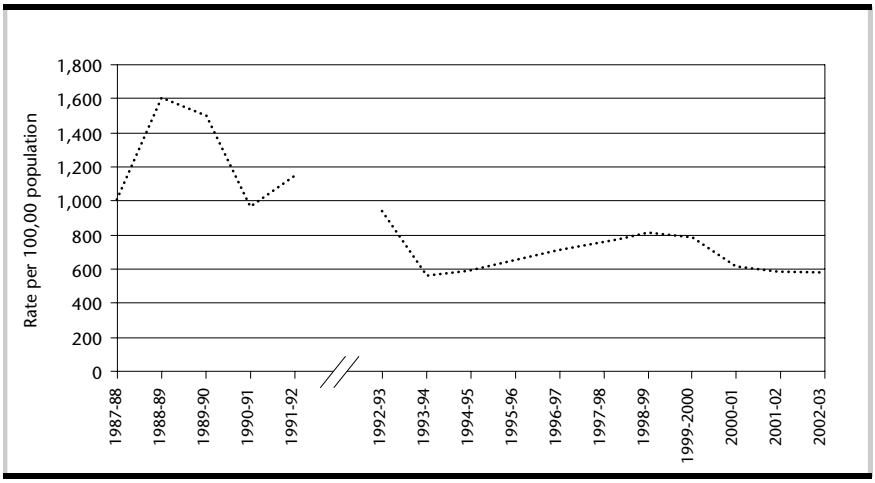
To understand the reasons for changes in the number of recorded offences it must be remembered that the population of Victoria has grown over time, making any increase in the raw number of offences reported not directly reflective of crime trends. Rates of deception offences per 100,000 of the Victorian population are shown in Figures 3.2 and 3.3 below.

Figure 3.2: Rate of Victorian fraud offences per 100,000 population, 1960–84



Source: See notes to Appendix D for sources, raw data and definitions of offence categories used. Breaks indicate years in which statistics were unavailable or years in which counting rules changed.

Figure 3.3: Rate of Victorian fraud offences per 100,000 population, 1987–2003



Source: See notes to Appendix D for sources, raw data and definitions of offence categories used. The break indicates the year in which counting rules changed.

The large increase towards the end of the 1980s is due largely to the introduction of ANCO and the change in offence categories. In addition, this was a time of considerable change in the business world in Australia, which could have resulted in an increased incidence of dishonesty. One view is that crime follows opportunity, so a consequence of increased business activity in boom periods was the creation of increased opportunities for fraud. And when businesses started to fail, individuals sought to prevent financial disasters by taking risks that took them outside the law. In both cases the effects would not become apparent in criminal statistics for a number of years. These arguments were supported to some extent in the evidence received by the Committee from the Corporate Crime Liaison Group. It was submitted that the increase of fraud at the end of the 1980s was due to the overheating of the economy. When interest rates increased, and people could no longer service their mortgages, this may have resulted in increased fraud. It was also submitted that the increase in computerisation, and the corresponding decrease in internal controls, may have led to an increase in financial crime.[73]

The substantial reduction in reported frauds during the 1990s may be due to the extensive fraud prevention activities which business and government introduced in the early 1990s, as well as the reduction in opportunities for fraud due to the economic downturn. Since 2001, it appears that the rate of reported crimes of dishonesty has remained stable.

The way in which Victoria Police collect official statistics has recently been reviewed by the AIC and suggestions have been made as to how the level of accuracy of official statistics could be improved (Carcach & Makkai 2002).

73 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

Evidence to the Committee from Victoria Police was that efforts are being made to improve the detail of official statistics that are being collected to enable trends in crimes involving misuse of identity or plastic cards to be discerned. Changes have been recommended in the LEAP data collection form to enable these more precise trends to be discovered.[74] The Committee has recommended the establishment of a dedicated agency within Victoria Police that would specifically be responsible for the collection of detailed fraud statistics.

Recommendations

1a. The Committee recommends that the Attorney-General for the State of Victoria seek a review of the Australian Standard Offence Classification, to enable more specific information on fraud and electronic commerce-related offences to be identified.

1b. The Committee recommends that the Attorney-General for the State of Victoria also request the Australian Bureau of Statistics to include fraud and other deception offences in its regular surveys of household and personal victimisation.

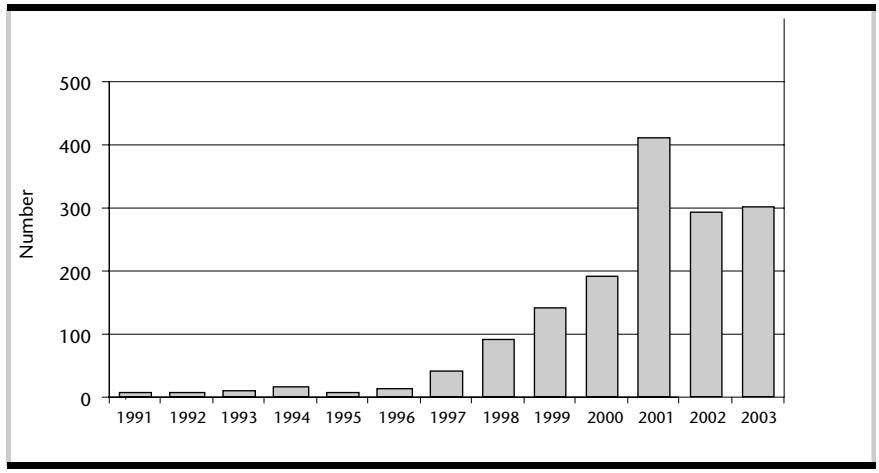
1c. The Committee recommends that any changes made to the Australian Standard Offence Classification be reflected in statistics that are collected and published by police, courts and correctional agencies in Victoria.

Official electronic crime statistics

Comparable statistics do not exist for crimes of dishonesty relating to electronic commerce, as there is no single offence category dealing with crimes of this nature. Of some relevance, however, is the increase in reported instances of general computer crime over the last few years. For example, the number of electronic crime referrals received by the Australian Federal Police has increased substantially in recent years, although there has been a slight decrease recently, as is apparent in Figure 3.4 below.

74 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

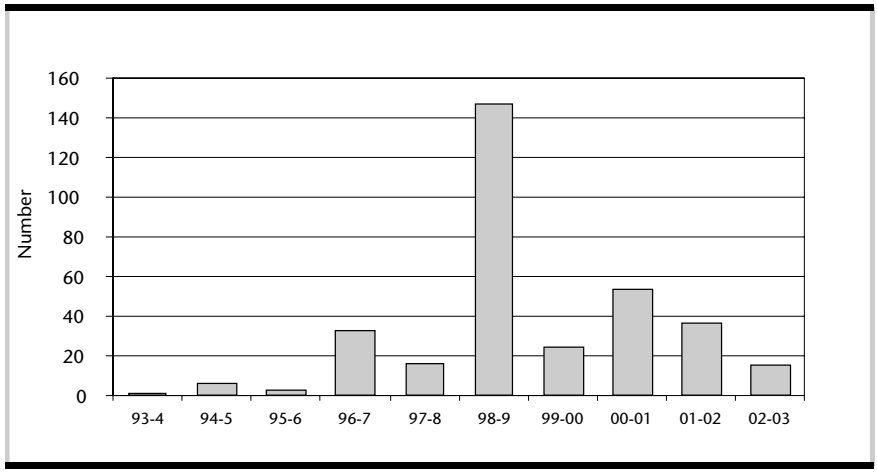
Figure 3.4: Electronic crime referrals received by the Australian Federal Police, 1991–2003



Source: Australian Federal Police 1991-2003, *Annual Reports,* Australian Federal Police, Canberra.

Recent Victoria Police statistics concerning computer-related crime in Victoria are set out in Appendix F of this Discussion Paper. Data shown in Figure 3.5 refer to computer-related offences officially recorded under Victorian legislation, rather than all matters referred for investigation as seen in Figure 3.4, and illustrate an increase since 1993/94. The large number of offences recorded in 1998/99 is due to a disproportionably high number of offences prosecuted in Victoria under federal legislation in that year.

Figure 3.5: Computer-related offences recorded by Victoria Police, 1993–94 to 2002–03



Source: Victoria Police 1993–2003, *Statistical Review of Crime 1993-94 to 2002-03*, Victoria Police, Melbourne.

Victorian regulatory agencies' statistics

Another indication of the extent of fraud can be obtained from statistics held by professional regulatory bodies in Victoria. Each year Annual Reports of the

Medical Practitioners Board (http://medicalboardvic.org.au/levelTwo.php?art=102&uid=2), the Dental Practice Board (http://www.dentprac.vic.gov.au/decisions.html), the Legal Practice Board (http://www.lpb.vic.gov.au/annual_reports.htm) and other statutory licensing authorities report cases in which complaints have been made concerning dishonest conduct allegedly engaged in by registered practitioners. Similarly, professional associations such as the Institute of Chartered Accountants in Australia and the Association of Certified Practising Accountants record allegations of fraud made against their members. Often, however, the way information is recorded makes it impossible to determine which allegations involve fraud and dishonesty, with organisations simply recording them as involving 'personal conduct', 'practice management' or 'offences'.

For example, in recent years the Medical Practitioners Board has classified complaints received into a number of different categories. One of these categories, known as 'offences', includes fraud, over-servicing and Medicare billing offences. In 2000/01 nine out of the 401 complaints referred to preliminary investigation fell into this category, while in 2001/02 there were 13 out of 573 (Medical Practitioners Board of Victoria 2002). However, as the 'offences' category also includes drugs and poisons offences, as well as other indictable offences, it is not possible to determine how many of these complaints specifically related to fraud. However, four of the 50 matters referred for Formal Hearings involved aspects of financial dishonesty, two of which resulted in the practitioner's registration being cancelled, one of which would have resulted in cancellation had the practitioner been present in Victoria, and the final case resulted in a reprimand being given (Medical Practitioners Board of Victoria 2002).

In previous years, when more specific information was provided in Annual Reports, the Medical Practitioners Board reported 10 out of 515 complaints of over-servicing fraud in 1995 and three out of 381 complaints in 1996. In 1995, two out of 57 informal hearings and none out of five formal hearings involved over-servicing fraud, while in 1996 three out of 88 informal hearings and two out of 30 formal hearings involved over-servicing fraud (Medical Practitioners Board of Victoria 1995, 1996). Similar information is available in other states (see, for example, Dix 2002 concerning New South Wales).

In 2000/01, the Legal Practice Board in Victoria received 95 claims representing over $4.2 million and conducted one prosecution against a conveyancer, resulting in a conviction and fine (Legal Practice Board 2001). In 2001/02, 60 claims representing over $4 million were received, with no matters being prosecuted (Legal Practice Board 2002).

Recommendations

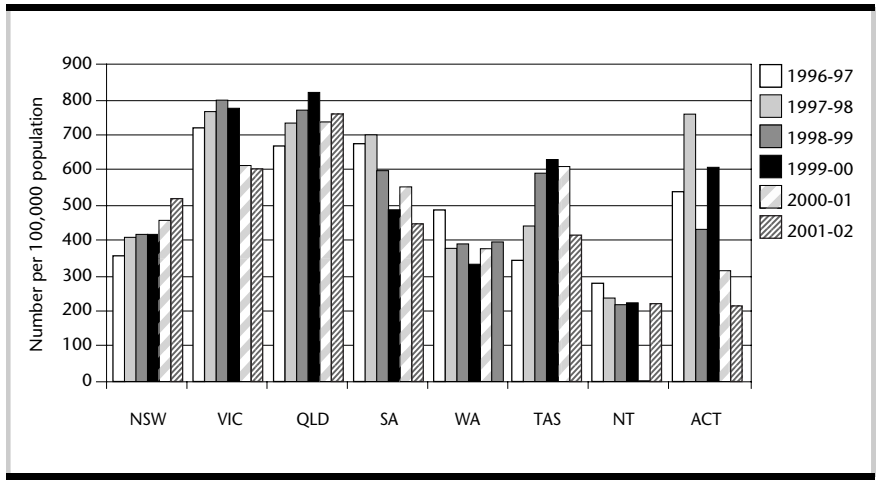
2a. The Committee recommends that legislation governing professional regulatory bodies, such as the Medical Practitioners Board of Victoria and the Legal Practice Board, be amended to require the annual publication of specific information about fraud and dishonesty-related complaints that have been referred for investigation, how those complaints were dealt with and the outcomes of investigations.

2b. The Committee recommends that all professional regulatory agencies be required to notify VFIRC of all matters involving fraud and financial crime or professional misconduct of a financial nature that come to their attention.

Comparison with other jurisdictions

Comparison between the various jurisdictions in Australia is difficult, not only because of differences in relevant offences and recording practices but also because of the limited availability of comparable statistics. Figure 3.6 gives a limited indication of differences between jurisdictions for the years 1996 to 2002, during which period Victoria experienced increasing rates of fraud offences reported to police until 1998/99, following which the rate has declined. Differences in rates between Victoria and other jurisdictions have to do with different fraud offence recording practices adopted by state and territory crime recording agencies, as well as underlying changes in the incidence of these crimes. In New South Wales, however, the rate of fraud offences has increased every year since 1996/97, although the overall rate has been lower than in Victoria. Queensland still shows the highest rate, followed by Victoria.

Figure 3.6: Fraud offences reported to Police for Australian jurisdictions, 1996–2002 (Rates per 100,000 population)



Sources: NSW: NSW Bureau of Crime Statistics and Research 1997–2003; VIC: Victoria Police, *Crime Statistics*, 1996/97–2002/03; QLD: Queensland Police Service, *Annual Statistical Review*, 1996/97–2002/03; SA: South Australia Police, *Statistical Review*, 1996/97 –2002/03; WA: Western Australia Police Service, *Annual Crime Statistics Report*, 1996/97–2002/03; TAS: *Annual Report of the Department of Police & Public Safety* 1996/97–2002/03; NT: Annual Report of the Police Force of the Northern Territory, Northern Territory Emergency Services, Fire Service of the Northern Territory/ Northern Territory Police, Fire & Emergency Services, *Annual Report* 1996/97–1999/2002/03 (Note: NT data were unavailable for 2000–2001); ACT: Australian Federal Police, *Annual Report on Policing in the Australian Capital Territory*, 1996/97–2002/03.

Fraud victimisation surveys

The nature and limitations of victimisation surveys

Unofficial statistical studies include victim surveys and surveys of offenders. These may be carried out by interview or through various forms of self-reported written questionnaires. Unlike official statistics that seek to canvass entire populations, unofficial surveys involve sample statistics in which a small representative group of subjects is examined and their responses used to predict the likely situation in an entire population. This, of course, introduces the possibility of error in the predictions made and the need for statistical controls to deal with this. There are also problems of reliability (whether repeated administrations of surveys elicit the same answers from the same subjects) and validity (whether the survey is measuring what it is supposed to be measuring).

One of the most significant problems with a victim survey of fraud offences is determining who is the appropriate person within an organisation to respond to the survey. The choice of a respondent who is sufficiently knowledgeable with respect to the circumstances of the offence is difficult, especially when managers are reluctant to engage in non-income producing activities. As Mr Dennis Challinger said in evidence to the Committee, failure to direct a survey to the correct person may lead to a very low response rate. For example, the response rate in KMPG's *Fraud Survey* (2002) was 18 per cent (361 out of

2,000), while the Association of Certified Fraud Examiners' *2002 Report to the Nation* (2002) had a response rate of 7 per cent (663 out of 10,000). However, these are quite large final samples.

The circumstances and complexity of the offence may also make the construction of a meaningful survey difficult. In complex frauds that extend over a long period of time, one individual may be unfamiliar with all the circumstances of the business. This may lead to telescoping of information (including events outside the survey period), exaggeration of facts, or selectivity of reporting, all of which are common problems with personal interviewing. There may also be problems of veracity where a manager is reluctant to report circumstances that may be incriminating either personally or for the business.

A further difficulty with victim self-report surveys is that the questions asked may be unclear, overly general or open to interpretation. In one survey, for example, subjects were asked:

> In the last twelve months, have you been the victim of fraud, forgery or false pretences? For example, have you been given a bad cheque, cheated out of money or property, or has your signature been forged?

This question clearly contains too many alternatives, each of which may be differently interpreted. It may be better to ask:

> In the last twelve months, have you been cheated out of money?

Subjects may also be unfamiliar with the legal definitions of offences, or may not consider that certain kinds of behaviour are criminal (such as tax evasion).

Victimisation surveys also often omit to deal with offences of dishonesty. The Australian Bureau of Statistics, for example, which conducts regular surveys of household and personal victimisation, fails to examine offences of deception and business fraud. The Committee has recommended (Recommendation 1b, above) that future surveys deal with such matters. Similarly, the International Crime Victims Survey does not deal with offences of fraud and dishonesty as a separate category (Van Kesteren, Mayhew, Nieuwbeerta & Bruinsma 2000).

Information on the extent of fraud victimisation is to be found in the business victimisation surveys conducted regularly by large consulting firms. Unfortunately the data are published in aggregate form, so it is impossible to identify trends as they relate to victims in Victoria specifically. Nevertheless, the results of these surveys have some relevance, as large corporations in Victoria are included in each of the samples.

KPMG fraud survey

KPMG's *Fraud Survey* (2002) examined 2,000 of Australia and New Zealand's largest organisations in September 2001. It received 361 replies (18%) with information being provided on fraud awareness, the experience and cost of fraud, who were the perpetrators of the fraud, how it was discovered, and why

it occurred. Information was also provided on action taken and fraud prevention steps relied on.

In all, some 44,654 incidents of fraud were reported as having taken place in the two years since the previous survey and 55 per cent of respondents reported at least one incident during that period. The reported incidence of fraud rose in proportion to the number of employees within the organisation. At least one fraud incident was experienced by 73 per cent of organisations with more than 1,000 employees and by more than 90 per cent of organisations with more than 10,000 employees.

Losses sustained by the 361 respondents amounted to $273 million, with the average cost for an organisation reporting fraud of $1.4 million.

Fraud perpetrators were divided into three categories: internal management, non-management employees and external parties. External parties were reported as being responsible for 91 per cent of the value of financial services frauds, although the majority of frauds not in this category were perpetrated by employees of organisations rather than by outsiders. Fraud perpetrated by internal management accounted for 28 per cent of the number of frauds committed by persons internal to the organisation, but for 67 per cent of the loss by value, as shown in Table 3.3.

Table 3.3: Perpetrators of major fraud

Perpetrator	Number of Frauds %	Value of Frauds %	Average Value of each fraud
Non-management employee	44	16	$82,890
Manager	29	51	$391,169
External party	27	33	$276,940

Source: KPMG 2002, *KPMG Fraud Survey 2002*.

Most instances involving outsiders related to credit card fraud, services and benefits obtained by false information and cheque forgery (89 per cent by number and 86 per cent by value). Categories of fraud by non-management employees causing the greatest losses were misappropriation of funds, false invoicing, and kickbacks or bribery, while 76 per cent of the value of all internal management frauds was traceable to misappropriation of funds or information theft.

The survey also found that six out of every 10 respondents admitted to having neither planned nor implemented appropriate fraud control strategies.

Ernst & Young survey

The firm of Ernst & Young has also undertaken fraud victimisation surveys of its clients since 1989. In its 7th global survey, conducted in October 1999, 11,000 senior executives in major organisations in 15 countries were surveyed, of whom 739 replied (Ernst & Young 2000). Of the 130 Australian respondents,

65 per cent reported having suffered fraud within the preceding 12 months, with just over one in 10 suffering more than 50 frauds. In the 8th global survey, conducted in 2002, approximately 50 per cent of Australian respondents reported having suffered fraud within the previous year, with fewer than 10 per cent of Australian respondents suffering more than 50 frauds that they were willing to disclose (Ernst & Young 2003).

In the 7th global survey, the single worst fraud suffered by all Australian respondents during the previous 12 months totalled an estimated $20 million, with only $5 million of that having been recovered (Ernst & Young 2000). Unfortunately, there were no equivalent data relating specifically to Australian respondents in the 8th global survey. Overall, 13 per cent of the worst losses were over US$1 million in amount (Ernst & Young 2003). In contrast to the previous survey, when only 29 per cent of losses were recovered, 51 per cent of losses were recovered in 2002. Only about 20 per cent of losses were recovered from perpetrators, however, with the remainder being recovered from insurers, banks and suppliers.

Both the 7th and 8th global surveys found the majority of frauds were committed by someone on the payroll. In the 1999 survey, 82 per cent of those who committed fraud were on the payroll, while in 2002 this number increased marginally to 85 per cent. However, in contrast to the 7th global survey, which found management to have committed only one-third of these frauds (with the remainder having been committed by employees), the 8th global survey found management to be responsible for 55 per cent of the frauds. Eighty-five per cent of these managers had less than one year's service in that position.

In the 7th global survey, 38 per cent of employee perpetrators of serious frauds were prosecuted and 28 per cent were dismissed. In 2 per cent of cases, no action was taken against employee perpetrators, while in the remaining 32 per cent of cases, employees were reprimanded, resigned, downgraded or other action was taken. No equivalent data were included in the 8th global survey.

PricewaterhouseCoopers surveys

In 2003 PricewaterhouseCoopers in conjunction with Wilmer, Cutler and Pickering (2003) conducted 3,623 interviews with senior managers of the top companies in 50 countries. Over 1,284 companies reported losses due to economic crime in the last two years with 813 of these companies able to quantify their loss. Some 37 per cent of respondents reported significant economic crimes during the previous two years with the average loss per company of US$2,199,930. Asset misappropriation was the most widely reported crime and was also the easiest crime to detect, with 60 per cent of all victims citing this as one of the frauds they had suffered. The biggest concerns for the future were asset misappropriation – the most visible of economic crimes – and cybercrime.

Also in 2003, the results of a study by the Australian Institute of Criminology and PricewaterhouseCoopers (AIC/PwC 2003) were reported. This study examined 155 completed files relating to 208 accused persons from each of the Australian states and territories as well as the Commonwealth and New Zealand (10 jurisdictions in all) relating to 165 males and 43 females, 183 of whom were convicted of offences. The study focused on cases involving 'serious fraud'. Files were mostly selected by the police and prosecution agencies concerned, in accordance with the criteria of seriousness of the fraud involved and year of determination. 'Seriousness' was defined on the basis of the following criteria:

- financial loss (generally over $100,000 unless other factors made the case of unusual seriousness or complexity); and/or
- sophistication in the planning and or execution of the offence (such as through the use of computers, electronic transfers of funds, forged instruments, multiple false identities etc.); and/or
- organisation of the offender(s) (such as the presence of multiple offenders, cross-border activities relating to the movement of individuals or funds, large numbers of victims etc.); and/or
- fraud offences committed by professionals such as solicitors, accountants, financial advisers, mortgage brokers etc. who carry out serious offences involving breach of trust concerning clients' funds.

The most common type of fraud involved obtaining finance or credit by deception (21% of offence types) followed by fraud involving cheques (15%), with a large number of cases involving cheques being prosecuted in Victoria. Dishonesty in obtaining government benefits occurred frequently in Commonwealth matters. By far the largest number of cases involved the victimisation of organisations in the financial services sector (36% of victims), followed by offences perpetrated against Commonwealth public sector agencies (13%). The financial services sector was the most victimised group largely because the most frequently occurring type of fraud involved abuse of credit and financial products. Computers were used in the commission of offences in only 20 per cent of files (31 cases). The relatively low incidence of the use of computers could be explained because some of these offences took place a number of years prior to being dealt with in the courts in 1998–1999. Indeed, some cases involved criminality perpetrated in the early 1980s when computers were a much less central part of business than they are today.

With respect to the characteristics of accused persons, it was found that they tend to be in their mid-40s, male, born in Australia, have completed secondary education or some professional qualification, are a director of a company or involved in accounting duties within an organisation, have relatively stable employment with the victim organisation, no prior criminal record, and act alone in the commission of the offence.

The two primary motivations for the commission of offences were the desire for personal advancement in the form of greed and gambling-related factors, with financial strain in individuals' personal and business lives also providing strong motivation. The most frequently identified rationalisations offered related to the intention to conduct a business legitimately in the future and the desire to repay the sums stolen. Admitting guilt, being remorseful and co-operating with the police were regularly identified factors raised in mitigation by offenders.

Three measures of cost were calculated for each case. First, the maximum amount included in final charges in respect of which the offender was sentenced, including sums taken into consideration for sentencing (*amount sentenced)*. Secondly, the amount of money the offender (or others on behalf of the offender) had repaid prior to the date of sentencing (*amount of restitution*). Thirdly, the maximum amount in respect of which the offender was sentenced, less any sums repaid by way of restitution (as explained above) or recovered by the victim through other forms of compensation, insurance, or professional indemnity payments made prior to sentencing, but excluding any indirect losses suffered by victims and losses incurred in prosecuting the case (*actual loss)*.

Over the two years in question, the 155 files involved $260.5 million in respect of the total amount sentenced, $13.5 million recovered as restitution prior to sentencing, and $143.9 million suffered as the total amount of actual loss. The maximum amount sentenced in any one case was $80 million. The largest losses were sustained in Queensland, with the Commonwealth, New Zealand, New South Wales and South Australia all involving losses in excess of $2 million each. In Victoria, the total amount sentenced was $1,654,826, the total amount of restitution made was $71,297, while the total loss was $715,828 over the two years in question. When these figures are compared with the mean for all jurisdictions they show that Victoria suffered less loss overall (the mean amount sentenced was $1.7 million for each file, offenders paid approximately $100,000 in restitution per file on average, and victims suffered a mean actual loss of some $941,000 per file) (AIC/PwC 2003).

Intellectual property loss surveys

Surveys have also been carried out to determine the extent of intellectual property loss sustained by business, which is one important component of white-collar crime. In June 2001, PricewaterhouseCoopers (2002) conducted a survey of 1,200 of Australia's largest private and public sector organisations to determine the nature and extent of intellectual property losses in Australia. One hundred and fourteen responses were received (approximately 10%). Almost one-third of respondents had experienced at least one intellectual property loss incident (108 incidents of loss were reported by the 114 respondents). Copyright breach was the most common method of acquiring intellectual property (29%), followed by trademark infringement (26%) and theft (19%).

Customer lists and data were the most frequently reported category of property stolen, followed by research and development.

Some 82 per cent of respondents reporting an incident were unable to report a known loss (18% reported incidents involving financial losses). Actual losses in Australian dollars ranged from $500 to $300,000 with an average loss of $46,000. The potential financial impact was estimated by 26 per cent of respondents to be between $1,000 and $5 million with an average potential impact of $1 million.

In 1999, the International Intellectual Property Alliance (2001) estimated that infringement of copyright laws in Australia occurred in respect of 4 per cent of total sales of motion pictures and 32 per cent of business software sales, constituting a total loss to the industry of US$143 million. More recently, the Australasian Film and Visual Security Office reported that the Australian cinema and video industry lost approximately $100 million to piracy in 2002, with an additional $60 million lost to pirated video games. The illegal market in Australia is now estimated to amount to 8 per cent of motion picture sales (Urban 2003). Unfortunately, Victoria-specific data were not available.

Identity-related fraud surveys

In recent years there have been a number of surveys designed to quantify the extent and losses involved in identity-related fraud. In the study undertaken by the Australian Institute of Criminology and PricewaterhouseCoopers (2003) of serious fraud cases prosecuted in Australia and New Zealand, it was found that false documents were used in the vast majority of cases, to support false claims in 69 per cent of matters (107 cases). False documents were used to provide evidence of a false or stolen identity, or with respect to false accounting practices, such as the use of false entries in ledgers or forged cheques. Fictitious identities (involving the creation and use of an entirely fabricated new identity) were used in approximately one-quarter of files, and stolen identities (involving the use, without authorisation, of a real person's name or other identifying information) in 13 per cent of the 152 files where information on false identity was available. Of the 152 files examined, 54 (36%) involved the misuse of identity in some way. The majority of files in which false names or identities were used entailed the use of one or two false names or identities, although one file involved an offender using 116 different names or identities. This proliferation of false identities is made possible by the use of desktop publishing equipment, now readily available to anyone with basic computing expertise and modest funds.

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

The other recent study of identity fraud was conducted by the Securities Industry Research Centre of Asia-Pacific (SIRCA) in 2003 (Cuganesan & Lacey 2003). This involved the calculation of the cost of identity fraud in Australia based on qualitative and quantitative data supplied by 120 organisations. Based on the data received, which did not examine individual identity fraud experiences of victims, it was estimated that in 2001/02 identity fraud cost $1.1 billion in Australia (see discussion below).

In addition, the SIRCA study found that less than 10 per cent of identity fraud events detected by organisations which provide and/or collect services and benefits were reported to police. Those organisations that actually issue documents used as evidence of identity, however, reported on average 19 per cent of events to police. Of those reported cases, between 46 per cent and 63 per cent were solved. On average, between 46 per cent and 55 per cent of fraud offences contained identity fraud-related events (Cuganesan & Lacey 2003).

Australian small business crime survey results

Information on some types of fraud perpetrated against certain retail businesses was collected at the end of 1999 for the AIC's *Small Business Crime Survey* via a postal questionnaire devised with the assistance of the Council of Small Business Organisations of Australia. The questionnaire was sent to about 28,000 randomly selected small businesses across Australia within a restricted set of sectors generally thought to have higher crime risks. Business owners/managers were asked to recount experiences of crime during the 1998/99 financial year. The response rate was 16 per cent. This yielded a sample comprising cafes/restaurants/take-aways (51%), general stores/milk bars (8%), liquor outlets (13%), service stations (11%), newsagencies (9%) and pharmacies (8%). Micro businesses (less than five full-time employees) comprised 56 per cent of the weighted sample, while small businesses (five to 19 full-time employees) comprised 44 per cent (see Taylor & Mayhew 2002b).

The data in Table 3.4 include two categories of fraud-related offences: cheque/credit card fraud and employee fraud. Although relatively small proportions of incidents were reported to police, these categories of fraud are of some importance to small businesses.

Table 3.4: Small business crime survey – Australian statistics

Type of crime		Attempted crimes			Completed crimes		
	Percentage victimised	Number of incidents	Number reported	Percentage reported	Number of incidents	Number reported	Percentage reported
Armed robbery	6	77	76	**98**	272	270	**99**
Burglary	27	1,052	762	**72**	1,342	1,308	**97**
Unarmed robbery	3	57	43	**75**	117	111	**95**
Theft of motor vehicle	3	64	23	**36**	101	88	**87**
Theft from vehicle	4	47	10	**21**	250	139	**56**
Owner/employees assaulted or threatened	7	402	66	**16**	636	282	**44**
Cheque/credit card fraud	10	716	108	**15**	1,903	483	**25**
Employee fraud	2	64	13	**20**	242	29	**12**
Customer theft	21	12,603	2,131	**17**	14,594	1,227	**8**
Employee theft	8	694	12	**2**	1,777	119	**7**
Bribery/extortion	1	67	3	**4**	13	3	**23**

Source: Australian Institute of Criminology 1999, *Small Business Crime Survey* [computer file].

Data from the *Small Business Crime Survey* relating to fraud offences reported by the Victorian respondents are presented in Tables 3.5 and 3.6.

Table 3.5: Small business crime survey – Victorian statistics for employee fraud

Industry ($)	Number of Victims	Number of Incidents	Total Direct Losses ($)	Total Indirect Losses
Retail Food (N=383)	2	2	3,000	4,000
General Stores (N=67)	1	10	30,200	0
Liquor Outlets (N=55)	0	0	0	0
Service Stations (N=159)	4	4	3,000	500
Newsagencies (N=147)	6	105	20,000	11,000
Pharmacies (N=152)	2	2	25,000	150
Total (N=963)	15	123	81,200	15,650

Source: Australian Institute of Criminology 1999, *Small Business Crime Survey* [computer file].

Table 3.6: Small business crime survey – Victorian statistics for cheque/credit card fraud

Industry	Number of Victims	Number of Incidents	Total Direct Losses ($)	Mean Indirect Losses ($)
Retail Food (N=383)	9	22	565	20
General Stores (N=67)	8	16	3,375	100
Liquor Outlets (N=55)	16	70	7,027	2,100
Service Stations (N=159)	11	353	16,050	2,290
Newsagencies (N=147)	6	320	12,318	100
Pharmacies (N=152)	14	22	2,424	625
Total (N=963)	64	803	41,759	5,235

Source: Australian Institute of Criminology 1999, *Small Business Crime Survey* [computer file].

Newsagencies were found to report the most employee fraud, while service stations and newsagencies reported the greatest number of cheque/credit card fraud. The total losses for these two types of fraud was $122,959 or $1,556 per victim and $132 per incident (see also Taylor & Mayhew 2002a). Although these losses seem relatively small in comparison with fraud losses experienced by larger corporations and government agencies, they have an important impact on small businesses which may have very narrow profit margins.

Deakin University/Victoria Police survey

In 1994 Deakin University in conjunction with the Victoria Police Major Fraud Group conducted a survey of fraud victimisation experiences of 477 medium (31%) or large (69%) businesses in Victoria (Deakin University 1994). Data were collected on 22 fraud categories, the most frequently mentioned being misappropriation of stock and equipment (251 cases – 53% of respondents) and misappropriation of cash (151 cases – 34% of respondents). Losses for these two categories over the five years examined were estimated to be $95,409,700 and $284,671,810 respectively. In total, respondents reported losses of $996 million for the five years in question (1989–94), or approximately $200 million per year. Some of the variables examined included whether the fraud was reported to the police, reasons for not reporting to the police, type of offender, factors contributing to the fraud, how the fraud was detected, and value of money lost.

Australian survey of crimes against businesses

As part of the International *Crimes Against Businesses Survey*, the AIC co-ordinated the *Australian Survey of Crimes Against Businesses* (Walker 1994) in which 966 Australian businesses were surveyed on a range of crimes experienced during 1992. Of particular relevance to this Inquiry were the questions that asked:

a) if the respondent had been the victim of employee fraud (anyone working for the company cheating the company by diverting funds, goods or services to their own purposes), and

b) if the respondent had been the victim of outsider fraud (fraud committed by outsiders, for example customers, distributors or suppliers, such as cheque and credit card fraud, under-deliveries etc).

Twenty per cent of respondents were victimised by outsider fraud and 6 per cent of respondents by employee fraud in 1992. Some 30 per cent of employee fraud incidents were reported to police.

The results of the sample surveyed were extrapolated to all businesses in Victoria. The weighted data on victimisation for all businesses in Victoria indicated that 20.8 per cent of businesses in Victoria were victimised by outsiders and 2.1 per cent by employees. Together, 22.9 per cent (16,016 Victorian businesses) suffered fraud in 1992, involving approximately $12.2 million.

Electronic crime and eFraud surveys

Business eFraud surveys

Several surveys have been conducted to ascertain the level of fraud risk associated with electronic commerce and the use of digital technologies generally. Again, these unfortunately fail to provide information specific to Victoria.

In relation to the influence of security risks on electronic commerce, in 2000 KPMG conducted the *Global eFraud Survey*, which surveyed more than 14,000 senior executives in large public and private companies in 12 countries. Responses were obtained from 92 companies in Australia. In total, 1,253 responses were received (KPMG 2001).

The survey found that 39 per cent of the 1,253 respondents said that security and privacy issues prevented their company from implementing an electronic commerce system, with 50 per cent of respondents saying that cost was the main problem in establishing such a system. Seventy-nine per cent of respondents indicated that a security breach to their electronic commerce system would most likely occur via the Internet or other external access. When asked to name the primary type of damage risk associated with their electronic commerce system, 72 per cent of respondents identified risk of damage to the company's reputation.

In KPMG's *Global eFraud Survey*, only 9 per cent of respondents indicated that a security breach had actually occurred within the preceding 12-month period, although 23 per cent of respondents from India reported a security breach of their electronic commerce systems, the highest percentage of any country surveyed. The types of security breaches reported included viruses, system

crashes, web site defacement or alteration, and system resources being re-directed or misappropriated. In approximately one-half of cases the victim was unable to identify the perpetrator (KPMG 2001).

KPMG also regularly conducts global fraud victimisation surveys, as discussed above. Between 1997 and 1999 the percentage of respondents who reported computer-related fraud rose from 7 to 12 per cent, a 71 per cent increase. Total reported losses due to computer crime were over US$16 million in KPMG's 1999 survey. However, these figures are likely to be underestimates, as many organisations were unable to quantify the extent to which they were being defrauded through the use of computers. Other organisations did not define some forms of fraud as computer-related (such as ATM fraud and false identification fraud carried out through the use of desktop publishing equipment). In 1999, 36 per cent of KPMG's respondents who reported computer crime were either unaware of how much they had lost or were unwilling to disclose it (KPMG 1999).

Of the 130 Australian organisations surveyed by Ernst & Young in October 1999, almost 60 per cent believed that computer fraud was likely or very likely to occur, particularly fraud arising out of the misappropriation of assets through the use of computers. The kinds of computer fraud that caused the greatest concern were those involving manipulation of data records or computer programs to disguise the true nature of transactions, theft or manipulation of business information by hackers (Ernst & Young 2000).

In November 1998, Victoria Police and Deloitte Touche Tohmatsu carried out a survey of 350 large Australian organisations (1999). Thirty-three per cent of respondents reported unauthorised use of their computers within the preceding 12-month period and one-quarter of these attacks were motivated by financial gain. More than one-third of those who responded believed that computer theft would have an impact on their organisation in the coming five years.

In early 2002, the Computer Security Institute and the FBI's Computer Intrusion Squad based in San Francisco released the seventh *Computer Crime and Security Survey* (Computer Security Institute 2002). This was a survey of over 500 computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities in the United States. Ninety per cent of respondents (primarily large corporations and government agencies) detected computer security breaches within the preceding 12 months, up from 85 per cent the previous year. Eighty per cent acknowledged financial losses due to computer breaches (64% the year before). Forty-four per cent (223 respondents) provided quantification of their financial losses, which came to US$455,848,000. In the previous year, 35 per cent (186 respondents) reported total losses of US$377,828,700, and the losses from 249 respondents in the 2000 survey totalled only US$265,589,940. The average annual loss reported over the three years prior to 2000 was US$120,240,180.

As in previous years, in 2002 the most serious losses occurred through theft of proprietary information and financial fraud. For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%). Thirty-four per cent of respondents reported the intrusions to law enforcement agents. In 2001 the figure was 36 per cent; in 2000 it was 25 per cent and in 1996 it was just 16 per cent.

In terms of reported incidents relating to electronic commerce, the survey found that 98 per cent of respondents maintained web sites, and 38 per cent suffered unauthorised access or misuse within the preceding 12 months, while 21 per cent said that they did not know if there had been unauthorised access or misuse of their sites. Twenty-five per cent of those acknowledging attacks reported between two and five incidents, while 39 per cent reported 10 or more incidents. Twelve per cent reported theft of transaction information and 6 per cent claimed financial fraud (8% in 2001, 3% in the 2000 survey).

Although solely based on corporations in the United States, these figures give some indication of the likely risk levels that might occur in Australia as computer usage rates approach those currently prevailing in the United States.

The Australian Computer Crime and Security Survey (2003) found that 42 per cent of the 214 public and private sector organisations surveyed reported some level of computer crime or abuse in the preceding 12 months, considerably fewer than the 67 per cent of respondents who reported attacks in the comparable 2002 survey. Possible reasons for this decline may include the fact that a larger sample was present in 2003 and that the definition of computer security incident was more stringent than in 2002. As in the 2002 survey, the most prevalent source of attack was the Internet (60% in 2003) with viruses representing the most common type of attack (80% in 2003). As in 2002, the two highest economic losses arose out of theft of Laptops and virus attacks, each accounting for over A$2 million aggregate cost over the preceding 12-month period. Only financial fraud involved higher total losses in 2003, amounting to A$3.5 million lost by those 126 respondents reporting quantified losses (Australian Computer Crime and Security Survey 2003).

In addition, a survey carried out by the AIC of 1,078 randomly selected businesses from five different categories of business across Australia – florists, booksellers, recorded music retailers, toy and game retailers and computer hardware retailers – found that between 30 and 40 per cent of online businesses within each business type had experienced online credit card fraud in 2002 and that preventive strategies tended to be implemented after an incident of fraud had been experienced. Knowledge of online credit card fraud liability also tended to be higher for those who had experienced fraud than those who had not. Of retailers within the five business types currently trading online (N=841) the following had experienced at least one incident of online credit card fraud since trading online: 43 per cent of booksellers; 33 per cent of toy and game

retailers; 30 per cent of computer hardware retailers; 28 per cent of florists, and 26 per cent of recorded music retailers. Overall, one-third of all business proprietors who have ever sold products online have been the victim of this crime at some stage and the total losses suffered by online retailers in 2001 and 2002 were $108,127 and $136,808 respectively. Booksellers experienced the most substantial loss per victim out of the five business types in both 2001 and 2002. Individual losses were quite high (some booksellers retail antique goods which, if fraudulently obtained, would involve a large charge-back amount), resulting in an overall higher level of loss for booksellers (Charlton & Taylor 2003). Once again, the results of this study do not differentiate between Victoria and the other states and territories in Australia.

Consumer eFraud surveys

Several organisations monitor the incidence of fraud by providing a complaints reporting service rather than soliciting responses through questionnaire-based research.

In the United States during 2002, the Internet Fraud Complaint Center, organised by the United States Department of Justice and the Federal Bureau of Investigation, received 75,063 complaints relating to matters such as auction fraud, credit/debit card fraud, computer intrusions, spam and child pornography. Of these, 48,252 were fraud complaints, a threefold increase from the previous year. US$54 million was lost in relation to these fraud cases, a $37 million increase from 2001. The average (median) monetary loss per referred complaint was US$299.00, with 46 per cent of complaints relating to auction fraud (Internet Fraud Complaint Center 2003).

The Federal Trade Commission's fraud database, 'Consumer Sentinel', which compiles identity theft and consumer fraud data from United States and Canadian agencies, recorded over 380,103 fraud and identity theft complaints in the calendar year 2002 (Federal Trade Commission 2003). This compares with 220,089 complaints received in 2001 and 139,007 in 2000. The proportion of these complaints that relate to identity theft has increased over the past three years, from 22 per cent in 2000 to 43 per cent in 2002. Fraud complaints accounted for the other 57 per cent of complaints in 2002. Of these fraud complaints, 47 per cent were internet-related in 2002, compared with only 31 per cent in 2000.

Finally, in a telephone survey of 1,006 online consumers conducted for the National Consumers League in the United States between April and May 1999, 24 per cent said they had purchased goods and services online. However, 7 per cent, which represents six million people, said that they had experienced fraud or unauthorised use of credit card or personal information online (Louis Harris and Associates Inc. 1999).

Australia moved from fourth highest contributor to complaints registered by the Internet Fraud Complaint Center in 2001, to the third highest in 2002,

accounting for 0.6 per cent of complaints, behind the United States (92.9%) and Canada (2.5%). Others in the top 10 countries reporting Internet fraud were Great Britain (0.4%), Germany (0.3%), Japan (0.2%), Netherlands, Italy, India and France (0.1% each). The top countries from which perpetrators operated, of those cases where their location could be ascertained, were the United States (76.5%), Nigeria (5.1%), Canada (3.5%), South Africa (2.0%), Romania (1.7%), Spain (1.3%), Indonesia (0.9%), Russia (0.7%), Netherlands (0.6%) and Togo (0.5%) (Internet Fraud Complaint Center 2003).

Although Australia was not included in the top list of countries from which perpetrators operated in 2002, this does not mean that no such perpetrators exist in Australia. This can be seen if the Internet Fraud Complaint Center's Annual Report for 2001 is examined, in which Australia is ranked seventh (0.4%) on the list of countries from which perpetrators operated (Internet Fraud Complaint Center 2002). Procedures to allow inter-jurisdictional co-operation, including the facilitation by local authorities of foreign proceedings against Australian offenders, will probably need to be in place in order to secure the co-operation of other countries for investigations and prosecutions originating here. These statistics are obviously heavily weighted towards the North American and English-speaking segments of the online community, but the contents of and contrasts between these lists of countries point to the global nature of the problem.

The top 10 types of Internet fraud recorded by the United States Internet Fraud Watch between 1999 and 2002 are shown in Table 3.7.

Table 3.7: Top Internet frauds, 1999–2002

Fraud type	1999 (%)	2000 (%)	2001 (%)	2002 (%)
Online Auctions	87	78	70	90
General Merchandise Sales	7	10	9	5
Nigerian Money Offers	N/A	1	9	4
Computer Equipment/Soft.	1.3	1	2	0.5
Internet Access Services	2	3	2	0.4
Information Adult Services	0.2	1	2	<0.1
Work-At-Home	0.9	3	2	<0.1
Advance Fee Loans	0.2	2	1	<0.1
Credit Card Offers	N/A	0.5	0.5	N/A
Business Opportunities/Franchises	N/A	N/A	0.5	N/A
Travel/Vacations	N/A	N/A	N/A	<0.1
Prizes/Sweepstakes	N/A	N/A	N/A	<0.1

Source: Internet Fraud Watch 2003, *Internet Fraud Statistics*.

Web sites were by far the most common way in which consumers encountered fraudulent Internet offers (94% in 2002). Only 6 per cent of initial contacts were made via email in 2002 (Internet Fraud Watch 2003). In the previous three years, however, the number of initial contacts made through email had

increased (from 9% to 15%) (Internet Fraud Watch 2002). In some of the most frequently reported Internet frauds, many of the offers came by email: 97 per cent of Nigerian money offers; 24 per cent of work-at-home schemes; 28 per cent of bogus credit card offers; and 36 per cent of fraudulent business opportunities and franchises (Internet Fraud Watch 2002).

Table 3.8 shows the average dollar losses sustained in Internet fraud recorded by Internet Fraud Watch between 1999 and 2001. No breakdown for these specific categories has yet been reported for 2002.

Table 3.8: Average Internet fraud losses (US$), 1999–2001

Fraud type	1999	2000	2001
Online Auctions	284	326	411
General Merchandise Sales	465	784	730
Nigerian Money Offers	0	3,000	5,957
Computer Equipment/Soft.	580	724	1,048
Internet Access Services	438	631	535
Information Adult Services	–	310	209
Work-At-Home	383	145	121
Advance Fee Loans	–	881	1,121
Credit Card Offers	–	138	309
Business Opportunities/Franchises	–	–	10,147
Overall average loss per person	310	427	518

Source: Internet Fraud Watch 2002, *Internet Fraud Statistics*.

It can be seen from Table 3.8 above that the amount of money consumers lost to Internet fraud increased between 1999 and 2001, with the average loss per person rising from US$310 in 1999 to US$518 in 2001. A minor decrease was noted in 2002, with the average loss per person being $468 (Internet Fraud Watch 2003). Overall losses have, however, increased dramatically, more than doubling between 2001 and 2002 (from US$6,152,070 to $US14,647,933).

Differences in the methods of payment used by the victims of Internet fraud have also been noted, as is apparent in Table 3.9.

Table 3.9: Payment methods used in top Internet fraud categories (percentage annual type), 2000–01

Payment type	Online Auctions		General Merchandise Sales		Nigerian Money Offers		Computer Equipment/ Software		Internet Access Services	
	2000	2001	2000	2001	2000	2001	2000	2001	2000	2001
Money Order	48	34	25	20	–	–	24	18	7	5
Credit Card	6	27	28	41	–	10	27	38	37	50
Cheque	32	18	24	15	–	–	22	14	14	9
Debit Card	1	6	5	7	–	–	–	9	9	9
Bank Debit	1	5	2	5	100	70	5	7	13	19
Cashier's Cheque	7	4	5	3	–	–	8	5	–	-
Cash	3	4	3	3	–	–	–	–	–	-
Wire	1	2	4	4	–	20	13	6	2	2
Telephone bill	–	–	–	–	–	–	–	–	15	4

Source: Internet Fraud Watch 2002, *Internet Fraud Statistics*.

From Table 3.9, it can be seen that consumers are using their credit cards more online. In 2002, for the first time, credit cards overtook money orders as the most common way in which the victims of Internet fraud in the United States paid for their products or services, with 34 per cent using credit cards, compared with 30 per cent using money orders (Internet Fraud Watch 2003). The use of credit cards is, however, inconsistent, as can be seen in Table 3.9, with some categories showing a large increase in credit card use for payments, while others such as Nigerian money offers continue to show bank account debits and wire services as the most common way to pay (Internet Fraud Watch 2002).

Quantifying loss in Victoria

Estimates of the dollar value lost to fraud can be derived from each of the above statistical sources of information. The limitations inherent in each source of data also apply to the estimation of financial loss suffered, with the added difficulty that estimation of loss is often more difficult than simply counting the number of fraud incidents that occur and determining how much was lost for each.

The definition of 'loss' also raises difficulties as it could include the actual sum obtained by the offender, the cost of investigation and prosecution, cost of remedial action, and loss of reputation and goodwill for businesses. PricewaterhouseCoopers' *Global Economic Crime Survey* (2003), for example, found that the damage inflicted by economic crime extends far beyond direct monetary loss. Intangible assets including business relationships, staff morale, reputation and branding can also be undermined by fraud or the perception of fraud. One submission received by the Committee referred to the indirect and

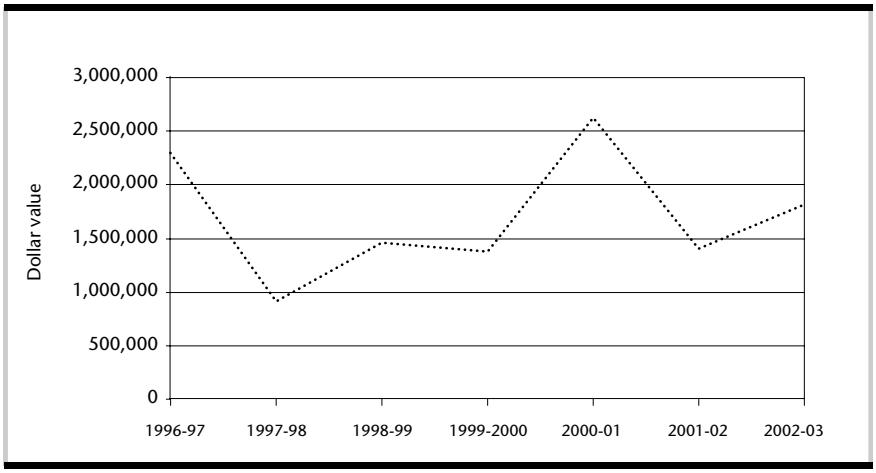
unquantifiable losses associated with fraud and also noted how many financial institutions write off millions of dollars each year as 'bad debt' rather than recording this as criminal fraud.[75] This obviously makes any estimate of loss based on official statistics extremely unreliable. Bearing these limitations in mind, the following figures are available.

Calculations based on official Victoria Police statistics

Victoria Police statistics have included estimates of the financial loss suffered by victims of fraud for many years now. Details of early estimates from the 1960s are set out in Appendix D showing total value stolen each year and average value stolen per offence. These data are estimates only and some offences recorded by police do not have losses reported. As one would expect, there has been a gradual increase since 1960, with some years showing substantial variations from previous years.

Data relating to certain offences were extracted from the LEAP database by Victoria Police Statistical Services Section and are shown in Appendix E. Figure 3.7 shows the total value stolen in respect of deception offences in which property was recorded as stolen or affected in Victoria since 1996/97, as recorded in Appendix E. These statistics differ from published data, which include additional fraud and deception offences (see Appendix D).

Figure 3.7: Victorian deception offences – Total dollar value stolen, 1996–97 to 2002–03



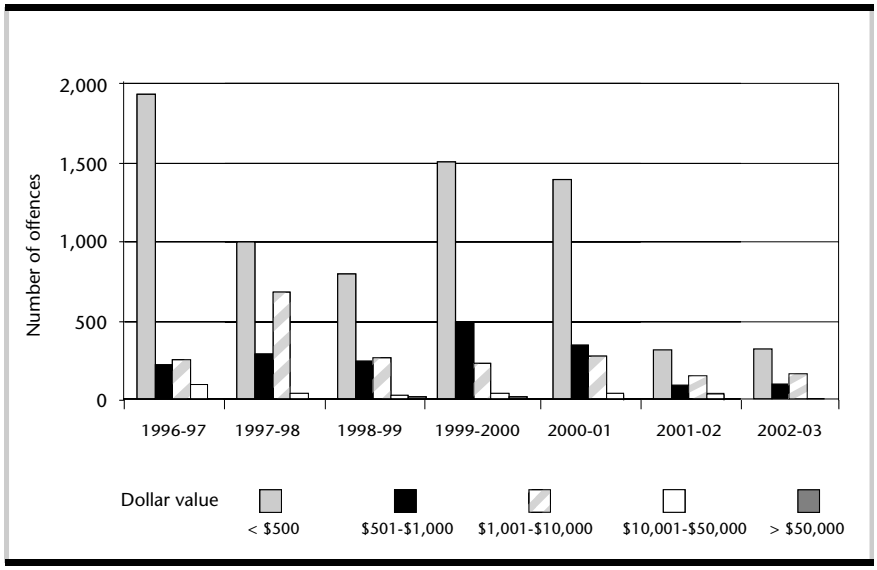
Source: Victoria Police 1996–2003, *Statistical Review of Crime,*Victoria Police, Melbourne.

Figure 3.8 shows changes in the value range of property affected in respect of deception offences recorded by Victoria Police since 1996/97 and extracted from the LEAP database (see Appendix E). The largest number of offences each year involved sums of less than $500 stolen or affected per offence

75 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

reported, with the number of offences involving such low-value amounts decreasing greatly since 2000/01.

Figure 3.8: Victorian deception offences – Dollar value stolen categories, 1996–97 to 2002–03



Source: Data provided by Statistical Services Department, Victoria Police 2003.

In 2002/03, published Victoria Police statistics (see Appendix D) showed that $1,824,989 was involved in deception offences recorded by police, or about $2,900 per offence. Using the finding in KPMG's *Fraud Survey* (2002) that only 62.6 per cent of fraud was reported to police, it could be estimated that $2.9 million was lost to all fraud incidents in Victoria in 2002/03. Clearly this total underestimates the full extent of fraud in Victoria considerably as it is not uncommon for individual fraud cases handled by the Major Fraud Investigation Division each to involve in excess of $1 million. This estimate also relies on the reporting rate found by KPMG, which related to a survey of only large corporate entities. The AIC's *Small Business Survey*, in contrast, found that between 12 and 25 per cent of the two types of fraud examined was reported to police. Applying these reporting rates to the reported loss of $1.82 million would result in estimated total losses of between $7.3 million (using 25%) and $15.2 million (using 12%).

A more sophisticated approach, also based on official statistics, is that developed by Mayhew (2003) who estimated that fraud cost the Australian community $5.88 billion in 2001. As Victoria has 24.8 per cent of the Australian population, it could be argued that fraud in Victoria could cost $1.45 billion, although this would assume that the incidence of fraud in all states and territories was uniform. It is, however, possible to use Mayhew's methodology to derive a more precise estimate of fraud costs in Victoria.

Mayhew began with the number of fraud offences recorded by police (in Victoria, this was 28,933 for 2002/03) and multiplied this by the average value per fraud offence which she took as $9,900. Mayhew then estimated that there were three undetected frauds for every one recorded and the average value of these undetected frauds was set at $1,600 per offence. (In Victoria, there would be 86,799 undetected offences.) An allowance was then made for a small number of very high value cases. In the AIC/PwC survey (2003) the 22 serious fraud cases examined in Victoria involved sums of $16,548,264 for the years 1998 and 1999 (averaging $8,274,132 each year, or $376,097 per large fraud offence). Using the same undetected rate of 3:1, the cost of undetected serious fraud cases would be $24,822,402. (The number of serious fraud cases was then deducted from the number of small fraud cases for both recorded and unrecorded). Added to this total was a 40 per cent weighting for lost output and intangible losses.

Using this calculation, the total fraud costs for Victoria would amount to $641 million as follows:

- 28,911 reported small fraud offences
  @ $9,900 per offence = $286,218,900
- 86,733 undetected small fraud offences
  @ $1,600 per offence = $138,772,800
- 22 reported large fraud offences
  @ $376,097 per offence = $8,274,132
- 66 undetected large fraud offences
  @ $376,097 per offence = $24,822,402
- add 40% of total for intangible losses
  ($458,088,230 x 1.4) = $641,323,520.

Calculations based on victimisation surveys

The various business victimisation surveys referred to above also include estimates of loss suffered by the victims of fraud. Only two of these surveys have data separately recorded for Victoria.

The Deakin University/Victoria Police Major Fraud Group survey of 477 medium and large businesses in Victoria found total losses of $996 million for the five years surveyed (1989–94) – approximately $200 million per year, or an average of $419,287 per organisation annually (Deakin University 1994).

The losses reported in the AIC's *Small Business Crime Survey* relating to employee fraud and cheque/credit card fraud offences reported by the Victorian respondents were $122,959 or $1,556 per victim and $132 per incident.

The extrapolated results from the *Australian Survey of Crimes Against Businesses* (Walker 1994) indicated that total costs of incidents in Australia in 1992, including security costs and stock losses, were between $3.8 billion and $4.7

billion. Of these costs, $235 million was attributed to fraud, with $190 million of this total being caused by outsiders and $45 million caused by employees.

The weighted data on victimisation for all businesses in Victoria showed that 20.8 per cent of businesses in Victoria were victimised by outsiders and 2.1 per cent by employees. Together, 22.9 per cent (16,016 Victorian businesses) suffered fraud in 1992, involving approximately $12.2 million. Using a multiplier of 30 per cent being reported to police, it could be estimated that $41 million was lost to fraud by all Victorian businesses in 1992.

KPMGs Australian *Fraud Survey 2002* found 44,656 fraud incidents reported by 361 organisations in the two years to September 2001, with losses of $273 million. Extrapolated to the 2,000 organisations surveyed, this totals $1.5 billion, with a $1.4 million average loss per organisation, or a $6,113 average loss per incident. KPMG also found that only 62.6 per cent of fraud was reported to police (KPMG 2002).

In 2002/03, 29,933 fraud offences were reported to police in Victoria. Using KPMG's reporting rate of 62.6 per cent, it can be estimated that 47,816 fraud offences may have been committed in Victoria that year. Using KPMG's average loss per incident of $6,113 per incident, this gives an estimated total loss of $292 million.

Calculations based on SIRCA study

Based on the data obtained in the study of identity fraud in Australia conducted by SIRCA (see above), it was estimated that in 2001/02 identity fraud cost $1.1 billion in Australia. Some 57 per cent of this ($626 million) involved the costs of resources consumed performing identity-related fraud response activities including risk assessment, deterrence, prevention and detection, as well as investigations, restoration and recovery. A further 38 per cent ($420 million) related to fraud losses actually incurred by users. Opportunity costs amounted to 5 per cent of the total ($56 million) – that is, resources spent on identity-related fraud responses that could have been deployed in generating income for the organisation (see Cuganesan & Lacey 2003).

Using population statistics, Victoria has 24.8% of the Australian population and so the Victorian proportion of the $1.1 billion cost of identity fraud, would be $274 million.

SIRCA also reported that some 50 per cent of Major Fraud Investigation Division cases in Victoria or New South Wales were identity fraud-related. In the AIC/PwC (2003) study of serious fraud, only 36 per cent involved the misuse of identity. Using the average of these two figures (43%), it can be estimated that the total cost of all fraud in Victoria would be $638 million. This figure approximates with that obtained using Mayhew's methodology above ($641 million).

Although each of the measures has certain difficulties and limited assumptions, it is likely that the cost of fraud in Victoria in 2002/03 would be in excess of $500,000 million.

Proposed reforms

Clearly the current state of information on the extent of fraud and electronic commerce-related crime could be greatly improved. Ideally there would be a single uniform computerised information system employed throughout all criminal justice agencies, including police, courts and corrections, which could be used for operational, strategic and statistical research purposes. Although the National Centre for Crime and Justice Statistics of the Australian Bureau of Statistics co-ordinates the collection of data from official criminal justice agencies, the data collected at present are by no means sufficiently focused to enable trends concerning fraud and deception to be discerned with clarity. If one is seeking information about specific methodologies of financial crime, such as identity-related fraud or credit card skimming, the position becomes even worse.

As noted, the Committee consulted widely on this question and, in view of the considerable benefits that could accrue through improvements in the collection of fraud information and enhanced levels of reporting, the Committee has determined that innovative proposals are called for, both to address concerns in Victoria and more generally throughout Australia. If the proposed reforms suggested for Victoria are found to be beneficial, then arguably these could provide a model for other jurisdictions to follow.

Victoria

In terms of the position in Victoria, the Committee suggests that a dedicated Centre be established within Victoria Police to co-ordinate and respond to all aspects of fraud reporting, prevention and the provision of information and statistics. It is suggested that a Victorian Fraud Information and Reporting Centre (VFIRC) be created that would fall within the infrastructure of Victoria Police, but be housed separately and centrally in order to facilitate easy access and to enhance visibility. The Centre would fall within the control of the Deputy Commissioner Specialist Operations, rather than the Deputy Commissioner Operations, as the Centre would not entail an investigatory function.

VFIRC would be staffed by civilian analysts with backgrounds in law, commerce, banking, statistics, and criminology, rather than sworn police officers. It would receive dedicated funding administered by Victoria Police, and seek to attract partial funding from the private sector.

VFIRC would not have a policing and intelligence function, but rather would be the central agency in Victoria for the collection and dissemination of information on fraud and financial crime and aspects of fraud prevention. It would also be the central agency in Victoria to which all reports involving

suspected fraud from members of the public as well as from public and private sector agencies should go. VFIRC analysts would receive reports, compile statistical information, and then transmit reports to the relevant agency or agencies for investigation as well as for victim support. For example, a complaint involving misleading and deceptive practices concerning the share market on the Internet could be referred to Victoria Police Major Fraud Investigation Division, the Australian High Tech Crime Centre, the Department of Business and Consumer Affairs Victoria, the Australian Securities and Investments Commission and other agencies at federal, state and territory levels. Officers at VFIRC would liaise with all relevant agencies to ensure that all cases that fell within individual agencies' jurisdiction were appropriately referred for investigation.

VFIRC should not, in the opinion of the Committee, be involved in the actual investigation of matters, and should not be located within the Major Fraud Investigation Division of Victoria Police. VFIRC analysts would, however, be required to follow the progress of individual cases through to prosecution and sentencing in order to enable complete data to be obtained concerning the outcomes of complaints (including prosecution, trial, sentencing, and appeal).

In relation to the public sector in Victoria, the Committee received evidence from Mr Wayne Cameron, Auditor-General of Victoria, that currently notifications on fraud by public sector agencies are provided to the Minister for Finance pursuant to the *Financial Management Act 1994* (Vic). The Auditor-General considered, therefore, that the Department of Treasury and Finance would be the appropriate agency for preparing an annual consolidated public sector return on fraud for Parliament's consideration. It was thought that this could form part of the Department's annual report. The Auditor-General further considered that:

> the emphasis in such a process would be on the compilation of meaningful macro data on the number, nature and value of fraud instances within each sector on a time series basis. The data would identify fraud committed by those who transact business with government (external fraud) as well as fraud perpetrated by those within government (internal fraud). Trend patterns, information on underlying causes, results of investigations and the nature of preventative action taken to avoid recurrences should form part of the annual communication to Parliament.[76]

In the Committee's view, however, VFIRC could play a role in gathering and analysing this information on behalf of the Department of Treasury and Finance, as under the Committee's proposal all fraud, whether perpetrated within or outside the public sector, would be required to be notified to VFIRC in the first instance.

76 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003. This formal submission was given to compliment evidence given by representatives of the Auditor-General on 6 October 2003.

Recommendations

3a. The Committee recommends the establishment of a Victorian Fraud Information and Reporting Centre (VFIRC), within Victoria Police, as a dedicated agency staffed by unsworn analysts, to:

i collect and disseminate information about the nature and extent of fraud occurring across Victoria;

ii collect and publish statistics on fraud; and

iii receive complaints of fraud from members of the public and public and private sector organisations for referral to appropriate agencies for investigation.

3b. The Committee recommends that VFIRC would not have an operational policing function in the investigation of cases of fraud. It should not be located within the Major Fraud Investigation Division of Victoria Police.

3c. The Committee recommends that VFIRC should be responsible for the collection and publication of statistics in relation to the nature and extent of fraud in Victoria, including information on prosecution and sentencing of fraud offenders.

3d. The Committee recommends that VFIRC should play a central role in relation to the reporting of fraud. All reports of fraud and financial crime in Victoria should be received by VFIRC either by direct notification from members of the public or as notified by other agencies.

3e. The Committee recommends that VFIRC should be located centrally in dedicated premises in order to facilitate access and to enhance visibility.

3f. The Committee recommends that VFIRC should receive a dedicated budget administered by Victoria Police.

3g. The Committee recommends that VFIRC should be the central Victorian agency responsible for the collection and analysis of reports of fraud perpetrated against public sector agencies in Victoria and by Victorian public servants. Individual government agencies in Victoria should be required to notify VFIRC of all cases involving suspected fraud that are required to be reported to the Minister for Finance. VFIRC analysts would then compile reports for the Minister for Finance as required under the *Financial Management Act 1994* (Vic.).

National

In terms of national reforms, the Committee supports the development of similar agencies to VFIRC in each state and territory. Information from these agencies could then be sent to a national body which would co-ordinate information as well as have a national fraud law enforcement function. To this end, the Committee recommends the establishment of an Australian Fraud Centre (AFC) which would provide a central information and intelligence

repository for all forms of fraud and financial crime. Ideally this could be housed within an existing national agency such as the ACC or the Australian Federal Police. Already the ACC has its National Fraud Desk which provides information and intelligence to law enforcement agencies throughout Australia. The AFC could usefully be developed out of the ACC's National Fraud Desk.

In addition to collecting criminal intelligence for use by law enforcement agencies the AFC would facilitate the exchange of trend information relating to financial crime. The Centre could also establish a web site, part of which could be accessible to private sector organisations and members of the public, and part could be a secure area that would facilitate the exchange of sensitive information and intelligence between law enforcement, government and relevant sections of the private sector on a variety of fraud-related issues.

Some of the operational aspects of the AFC would involve its ability to detail emerging trends in identity-related fraud, credit card fraud, plastic card skimming, telecommunications fraud and fraud against federal, state and territory agencies. The secure virtual private network would enable information to be recorded on suspects and offenders as well as criminal methodologies. This would permit the free flow of data between the Centre and participating agencies.

The public area of the site would provide general fraud awareness, prevention information, education and support strategies to respond to fraud risks and provide information on avenues of support for victims. For example, information could be provided on the nature of identity theft, common experiences of victims, who to contact, what to do as a victim, and how to make a complaint (see Chapter 10 for more information on victim support services).

The AFC could also maintain a Register of fraudulently used identities, a Register of victims of identity fraud to help law enforcement deal with cases of re-victimisation, a Register of stolen and lost documents used to establish identity, such as birth certificates and drivers' licences, and a database of images of legitimate documents used as evidence of identity (see Chapter 7). In addition, various other documents and intelligence relevant to fraud could be maintained.

Recommendations

4a. The Committee recommends the establishment of an Australian Fraud Centre (AFC), to collect and disseminate information about the nature and extent of fraud occurring across Australia and to help co-ordinate a national response to fraud. In order to facilitate the establishment of the AFC, the Attorney-General for the State of Victoria should propose its establishment at the next meeting of the Standing Committee of Attorneys-General.

4b. The Committee recommends that the AFC should be involved in the collection and dissemination of fraud intelligence and the publication of national fraud statistics.

4c. The Committee recommends that the AFC should be housed within the infrastructure of either the Australian Crime Commission or the Australian Federal Police.

Further research

Although considerable research has been undertaken to document the nature and extent of fraud in Victoria, there remains a need for further specifically targeted research activities. Ongoing fraud victimisation surveys are valuable for those in both the public and private sectors as a means of understanding new and emerging risk areas and also in directing resources to the most urgent areas of need. At present, however, there are few surveys that specifically target electronic commerce-related risks, as most surveys either deal with general fraud experiences or computer crime risks, of which electronic fraud forms only one component.

In addition, research is needed to examine specific areas of risk. The Committee has identified both the higher education sector as well as the gambling industry as worthy of further investigation in terms of these areas providing environments that create opportunities for crimes of dishonesty to occur (in the case of higher education) or to lead to the indebtedness of their patrons (in the case of gambling venues), which could then result in the commission of financial crime.

Recommendations

5a. The Committee recommends that surveys be conducted of businesses and companies operating in Victoria to determine the nature and extent of their fraud and electronic commerce-related victimisation.

5b. The Committee recommends that a study be undertaken in Victoria to determine the financial and indirect costs associated with fraud and electronic commerce-related crime in Victoria.

5c. The Committee recommends that research be undertaken to determine the nature, extent and financial cost of fraud perpetrated in the higher education sector in Victoria (including Tertiary and Further Education Institutes), and steps which can be taken to address this problem.

5d. The Committee recommends that research be undertaken to ascertain the links between fraud and gambling, and ways in which this issue can be addressed.

Conclusion

Although there is a good deal of information currently available concerning the extent of fraud and electronic commerce-related crime, there are certain limitations that prevent the size of the problem from being ascertained with precision in Victoria. Official statistics have the primary limitation that they deal only with matters that come to the attention of the police, while victimisation surveys often do not provide enough specific detail about the crimes of dishonesty with which this Inquiry is concerned.

On the basis of the information documented in this chapter, however, it is clear that crimes of dishonesty have increased in Victoria since the 1960s and that financial losses, even relating to officially reported matters, involve many hundreds of millions of dollars each year, perhaps even exceeding $500 million in Victoria alone. More precise quantification must await more targeted and extensive research that will require the co-operation of public sector agencies and organisations in the private sector. This will need a commitment to conducting such research and to sharing information publicly, within both government and the private sector. The creation of VFIRC would assist not only in the compilation of accurate information and statistics on fraud in Victoria, but also in improving fraud reporting and reducing the incidence of crimes of this nature through the wide-scale dissemination of fraud prevention information and advice. By having a more precise understanding of the scale of the problem of fraud in Victoria, fraud prevention resources could be allocated more effectively and new initiatives developed to control new methodologies of financial crime as they occur and, hopefully, to prevent them from being initiated.

4. Fraud Risks of Electronic Commerce

Introduction

Having examined the nature and extent of fraud and white-collar crime more generally, this chapter focuses on the fraud risks inherent in the use of technologies of electronic commerce. Before considering some examples of dishonesty involving electronic trading and communications, this discussion begins by examining the nature of electronic commerce and how it brings with it new risks. These risks predominantly relate to the lack of physical presence of people in transactions and the ability of people to disguise or manipulate their identity when conducting business online. The discussion will then turn to the various risks that arise for government, business and individuals in conducting business electronically. Unfortunately, many of these risks have already eventuated, while others have yet to be realised. The challenge is to design systems that will minimise risks while not impeding the efficient and expansive development of commerce.

The nature of electronic commerce

Loss of collateral information

As noted in Chapter 2, and as with other crimes, fraud can be understood as being a result of three interlocking factors: a supply of motivated offenders, the availability of suitable targets and the absence of capable guardians.

The growing number of individuals engaging in electronic commerce has led to an increase in the availability of suitable targets. Perhaps more worrying is the possible increase in the pool of motivated offenders. In their discussion of the psychology of fraud, Duffield and Grabosky made the following observation:

> While the degree of callousness required to dupe someone face-to-face is fortunately quite rare, far more individuals are capable of the depersonalised social aggression required for indirect fraud. In fact, it has been suggested that lack of social cues in communication such as email leads to a reduction in the influence of social norms and constraints on the average person's behaviour (2001, p.5).

Most electronic transactions entail a loss of collateral information about those involved, such as key social and business cues that are used to establish trust in commercial transactions including appearance, facial expression, body language, voice, dress, and demeanour. The absence of such cues greatly enhances the ability of offenders to disguise their identities or to make use of other people's identities, which is often an essential component of electronic crimes. The development of effective user authentication technologies may provide a solution to this problem.

In addition, the speed with which online transactions take place facilitates acts of fraud, as there may be no 'cooling-off' period during which the parties to transactions can reflect on the terms of a proposed agreement and obtain verifying evidence about the subject matter or identity of the other contracting party. Sometimes internal controls designed to prevent fraud may not apply to online transactions, in which agreements may be struck and payments made instantaneously.

Electronic commerce technologies

The technologies associated with electronic commerce provide many opportunities for individuals who wish to commit crimes of dishonesty. Fraud can occur by individuals transmitting misleading and deceptive information online, by failing to honour contractual agreements entered into electronically, or through the misappropriation of funds transmitted electronically. Theft of funds does not, however, involve simply stealing 'digital bags of money' as they pass along telephone wires, but rather entails the manipulation of instructions provided by users to debit or credit specified accounts (see Grabosky, Smith & Dempsey 2001, Chapter 2). Fraud prevention requires that the instructions given by the parties to a transaction – be they consumers, merchants or financial institutions – cannot be tampered with, assuming that such instructions are genuinely given by authorised parties in a fully informed state of mind.

Traditional payment systems

Various payment systems have been developed for use in connection with electronic commerce (see Smith & Urbas 2001). Some make use of telephone accounts that allow vendors to obtain access to purchasers' funds, while others make use of electronic cash in which value is held electronically on the computer's hard drive and debited or credited as and when the need arises. Newer forms of stored-value cards (usually involving computer chip technology) have been designed to record monetary value and may also be used to transfer funds from a bank's ATM to a personal computer and thence to a business. These systems are obviously more efficient, since transactions may be carried out and paid for instantaneously.

The simplest payment mechanism involves payment by cash or money order once an agreement has been reached electronically. In addition to paper-based

transactions, online payments could be made in two ways. The first is by way of direct debit, in which value is transferred directly from the payer's account to the recipient's bank, and the second is credit transfer, in which a payer advises the bank to debit his or her account with a sum that is then electronically credited to another account. These are essentially card-not-present transactions which operate in the same way as any credit card payment made by telephone or mail order. In order for such transfers to take place, preliminary steps need to be taken by the parties involved. These include the exchange of account details and the conduct of various identification checks.

Fraud has been greatly facilitated by offenders obtaining credit card account numbers from online services, such as Credit Master and Credit Wizard. These Internet sites generate large volumes of credit card numbers that can then be used to fraudulently order goods or services using the account of a legitimate cardholder. The sole purpose of these credit card generator programs is to aid in finding particular credit card numbers that merchants will accept as legitimate. By generating a large enough group of account numbers, offenders can make substantial fraudulent purchases of goods or services which, ultimately, the merchant will be required to pay for (Department of Justice, United States 1999).

Alternatively, credit card account numbers and other personal information can be misappropriated from databases maintained by organisations in both the public and private sectors. Some recent cases involved the removal of tens of thousands of credit card details from commercial enterprises. In the largest known case, a hacker stole 485,000 credit card numbers from an electronic commerce web site and secretly stored the information on an American government agency's web site (Lehman 2000). In another case, Creditcards.com was hacked, and 55,000 card numbers were to be retained until the offender received a payment of US$100,000, which he claimed from the victim company. When the extortion attempt failed, the hacker posted the card numbers on the Internet. The company has since created a web site at which merchants and customers can check for fraudulent transactions (Berinato 2000).

Electronic funds transfer systems

Various systems are being developed to enable customers, banks and merchants to communicate securely with each other. A number of electronic funds transfer systems already operate throughout the world as substitutes for paper-based cheque transactions and these could well be adapted for use in electronic commerce transactions. These systems create a security risk if procedures are not in place to verify the availability of funds to be transferred, or if account access controls are not in place. There is also the possibility of information being manipulated as it passes over the network in unencrypted form.

In order to secure electronic funds transfers, data are generally encrypted using algorithms that encode messages. These are then decoded using electronic keys

known to the sender and the recipient. The major security risk associated with such a system lies in the possibility of the encryption keys being acquired by a third party, in which case data within the system could be revealed or manipulated. Most of the large-scale electronic funds transfer frauds committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers of financial institutions (Meijboom 1988).

Smart card systems

Other organisations are considering the use of smart cards with the capacity to store value and transfer this to merchants via the Internet. Smart card payment systems may take a variety of forms. The system that most closely resembles the early forms of stored value cards involves a scheme operator that administers a central pool of funds. When a cardholder transfers value to the card, the funds are actually transferred to a pool controlled by the scheme operator. A merchant who is paid from the card takes evidence of the receipt to the scheme operator, which pays the relevant amount from the pool.

Yet other payment system proposals, such as those operated by MasterCard and Visa International, envisage a number of brands of cards being accepted. In such schemes there is no central pool of funds, instead each card issuer is responsible for reimbursing merchants that accept their cards. Various systems are also being developed which will permit transactions to be carried out securely on the Internet through the use of electronic cash, or value tokens that are recorded digitally on computers. In these systems, before purchases can be made, both the merchant and the customer need to establish banking arrangements and Internet links with the bank issuing the tokens.

The customer first requests a transfer of funds from his or her bank account into the electronic systems. This is similar to withdrawing cash from an ATM. The system then generates and validates coins that the customer is able to use on the Internet. The coins are data streams digitally signed by the issuing bank using its private key. The customer can then send electronic cash to any merchant who will accept this form of payment using the software provided by the service provider. The customer encrypts the message and endorses the coins using the merchant's public key. The merchant then decrypts the message with its private key and verifies the validity of the coin using the issuing bank's public key. Finally, the merchant presents the electronic cash to the issuing bank with a request for an equivalent amount of real funds to be credited to the merchant's bank account.

The (now defunct) Australian Commission for the Future (1996, pp.62–3) identified a number of ways in which frauds may be carried out through the use of smart cards. Concerns were expressed that card readers could be programmed to deduct greater value from the card than that authorised by the user, or to enable sales staff to intentionally deduct greater sums than they are authorised to deduct. Sums rounded off to the nearest five cents could also be

skimmed to the terminal owner's advantage. Finally, if stored value cards are stolen and are unprotected by a PIN, or the PIN can be compromised, the value may then be removed from the card. Other potential threats identified by the Australian Commission for the Future included the use of smart cards for money laundering and tax evasion as well as for fraud carried out through the use of counterfeit cards (1996, pp.74–6). More recent technological developments have solved a number of these concerns.

Public key systems

Public key authentication systems allow individuals and organisations, including government agencies, to conduct secure online transactions. They can also be used to authenticate subscribers to web pages and servers, and to ensure the integrity and confidentiality of information in the online environment. A framework exists for the generation, distribution and management of public key certificates that bind the identity of users to their public key material in a trusted and legally-based manner. In so-called PKI systems, users have two keys: a public key and a private key. The user may publish the public key freely. The keys operate as inverses giving rise to two results. Only the holder of a private key can decode a message someone else has encrypted with the corresponding public key. Also, a user can sign a message with a private key, and the signature can only be verified with the corresponding public key. These two mechanisms allow authentication of an individual, an organisation or a role, non-repudiation of messages, and secure transfer of information.

Digital signatures are cryptographic techniques that encrypt a hash or digest of a document with a user's private key. This creates a unique and unforgeable identifier that can be checked by the receiver to verify authenticity and integrity and provide non-repudiation. Digital signatures can function on electronic documents in the same way as physical signatures do on paper. This means they can be used to automate transactions that are currently carried out on paper. Digital signatures can be applied to email, Internet transactions, World Wide Web pages, EDI transactions and more (National Office for the Information Economy 2003).

The Australian government has developed a strategy, entitled *Gatekeeper*, that aims to provide a common platform for the development of systems that rely upon public key cryptography and digital signatures. The strategy seeks to provide a system of secure electronic communications on public networks when dealing with Australian government agencies. A trusted system of certification for the Australian government will enable verification and authentication of transactions between clients, industry, government agencies and other governments (National Office for the Information Economy 2003).

A Public Key Certificate is the information that identifies the Certification Authority issuing the certificate; identifies its owner; contains the owner's public key; and is digitally signed by the Certification Authority issuing it. To date,

Gatekeeper accreditation has been granted to nine organisations,[77] and a further two have sought accreditation.[78] For example, Digital certificates linked with encoded Australian Business Numbers (which are required for taxation purposes) are being used by the Australian Taxation Office and the Australian Securities and Investments Commission to permit lodgment of taxation returns and other company documents electronically. The Health Insurance Commission, which administers publicly funded health and medical services in Australia, has also issued its own digital certificates to permit secure electronic communications between health service providers and itself over the Internet.

The main security risks associated with these systems relate to the possibility that private encryption keys could be stolen or used without authorisation. One way to do this would be to submit false identification evidence to Registration Authorities when obtaining a public-private key pair. Alternatively, if a private key were held on a smart card it might be possible to obtain access by breaking the access control device on the card, which could simply be a password or PIN. Thus, someone could make use of another person's private key to order goods or services from the Internet, and be untraceable. To counter these possibilities, *Gatekeeper* has been amended to improve the evidence of identity required before key pairs are issued. Details of the amended *Gatekeeper* strategy are available from the web site of the National Office for the Information Economy.[79]

Mobile commerce

Recent technological developments now enable transactions to be conducted through the use of mobile telephones and messaging services. In June 2002, Consumer Affairs Victoria released a Discussion Paper examining Mobile Commerce ('M-Commerce') in which it considered the various regulatory challenges, security concerns and possible solutions from a consumer's perspective. M-Commerce was defined as the 'use of handheld wireless devices to communicate, interact, and transact via high-speed connection to the Internet'. Examples given included the use of wireless devices to gain access to banking accounts and pay bills, to receive stock quotes and to initiate, buy or

77 Australia and New Zealand Banking Group Limited – as a Core Registration Authority (ANZ has also achieved Gatekeeper Recognition); SecureNet Limited – as a Certification Authority; PricewaterhouseCoopers (beTRUSTed) – as a Certification Authority and Core Registration Authority (beTRUSTed is accredited to issue ABN-DSCs); Australia Post – as a Core Registration Authority; Telstra Corporation Limited – as a Certification Authority and Registration Authority – Extended Services (Telstra is also accredited to issue ABN-DSCs); VeriSign Australia Limited – as a Certification Authority and Core Registration Authority; Health eSignature Authority Pty Ltd – as a Registration Authority – Extended Services; Baltimore Certificates Australia Pty Ltd (CAPL) – as a Certification Authority; and the Australian Taxation Office – as a Certification Authority and Core Registration Authority (National Office for the Information Economy http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm).

78 Ozdocs International Pty Ltd and Queensland Government (National Office for the Information Economy, http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm).

79 National Office for the Information Economy http://www.noie.gov.au/projects/confidence/Securing/EOI%20Requirements.htm.

sell transactions, or to receive special promotions and to generate orders from any place at any time.

After considering the likely increase in M-Commerce over the next few years, the Discussion Paper describes the range of services available through mobile messaging services and the accompanying regulatory problems. M-Commerce exacerbates some of the fraud risks that arise in electronic commerce transactions using fixed-line connections such as those conducted from personal computers. The concern is that M-Commerce transactions might increase the impulsiveness and immediacy of transactions, and the absence of a cooling-off period could result in some consumers engaging in transactions that superficially appear sound but which in fact involve deception and are difficult, if not impossible, to undo.

An added concern relates to the theft of portable hardware such as mobile telephones and hand-held computers. Unless secured by appropriate authentication devices, a stolen phone could enable a thief to gain access to considerable amounts of personal information about its owner, including bank account numbers and other key identifying details. As the Discussion Paper notes:

> Securing m-commerce may be even more difficult than protecting wired transaction. Constrained bandwidth and computing power, memory limitations, battery life and various network configurations all come into play, raise [sic] the questions as to whether there will be adequate security for users without compromising the ease of use and speed.
>
> In the use of text messaging, a number of security issues have already been identified, and will extend to the use of m-commerce. While a direct SMS message is relatively safe because it is encrypted for its transition from one mobile handset to the other, because of its store forward nature, messages are vulnerable to being corrupted. Like voice messages, SMSs are stored on a server before being forwarded to the receiver. There is no mandatory encryption and access protection for storage. The only way to secure the entire transmission would be with end-to-end encryption.
>
> Messages exchanged between two service providers can also be violated in transit if the link between the two networks is not protected. If this information is payment details or authorities to make transactions, there is even more danger (Consumer Affairs Victoria 2002, pp.11–12).

A further concern noted in the Discussion Paper relates to the popularity of mobile technologies with young users who may be more easily targeted by criminals. Although young people may be familiar with the operation of new technologies, they might not be aware of some of the forms of dishonesty that can arise, and therefore be more vulnerable to victimisation (see section in Chapter 3, 'Fraud against consumers – Younger persons').

The outcome of the review by the Ministerial Council on Consumer Affairs of consumer issues to do with mobile commerce is due to be released some time in 2004 (Ministerial Council on Consumer Affairs 2003).

Electronic commerce usage surveys

The practice of quantifying the extent of fraud arising out of electronic commerce remains in its infancy, owing partly to the ongoing development of the technologies of electronic commerce, and partly to the absence of specific research addressing this issue. It is, however, possible to quantify the extent to which some of the technologies that support electronic commerce are being used and the likely level of risk associated with usage.

In Australia there were 554 Internet Service Providers (ISPs) supplying Internet access services to 5.1 million active subscribers at the end of March 2003. Of these, there were 4.4 million household subscribers and 659,000 business and government subscribers. There were 3,046 million megabytes (Mbs) of data downloaded by Internet subscribers during the March quarter 2003, almost two-thirds more than in the same quarter of 2002 (1,831 Mbs). Of this, household subscribers downloaded 2,264 million Mbs and business and government subscribers downloaded 782 million Mbs (Australian Bureau of Statistics 2003b).

These quantities of data are put into perspective when one considers that one thousand pages of text is approximately one megabyte of data (3,046 million megabytes of data would correspond to some 3,046,000 million pages of text). Of course, much of these data would comprise images and video files. A single JPEG image could contain up to three megabytes of data.

In Victoria, there were 187 ISPs at the end of the March quarter 2003, and 1,338,000 subscribers. In Victoria, 847 million Mbs of data were downloaded during the six months ending March 2003. In the same period, the number of ISPs decreased by 11, but the number of subscribers increased by 158,000. Data downloaded by Internet subscribers during the March quarter 2003 increased by 138 million Mbs from the September quarter 2002 in Victoria (Australian Bureau of Statistics 2003a).

More detailed usage statistics are provided by the other Internet usage surveys carried out by the Australian Bureau of Statistics (1998a, 1998b, 1999, 2000c). These showed an increase of 52 per cent in the number of adults who had gained access to the Internet between November 1998 and May 2000 – 4.2 million adults (31% of the adult population) to 6.4 million adults (46% of the adult population).

The surveys also found a 180 per cent increase in the number of adults who had used the Internet to purchase or order goods or services for their own private use between November 1998 and May 2000 – 286,000 adults (2.6%) in the 12 months to November 1998 to 802,000 adults (6%) in the 12 months to May

2000 (a 2.4% increase in the proportion of the adult population making private online purchases).

The percentage of Internet shoppers who paid for goods and services by disclosing their credit card details online stayed much the same, increasing from 80.5 per cent in November 1998 to 81 per cent in May 2000. Books/magazines and computer software/equipment were the most common types of goods or services (27% and 19% respectively) purchased from the Internet for private use in the year to November 1999 by adults in Australia.

The potential exists, however, for anything to be purchased electronically. Over the last year a number of higher-value transactions have been conducted electronically, with purchasers buying holidays, cars and even houses online. A number of online auction houses have also been established and the Internet is now used for online share-trading and gambling, all of which could soon involve much larger sums of money being transacted. Meanwhile, very high rates of low-value transactions seem likely to emerge as the practice of payment for online content becomes more widespread. It has been reported that Europeans spent £140 million on online content last year alone (BBC Online 2002).

In Australia, the National Office for the Information Economy's (NOIE) report *E-Commerce Beyond 2000* suggests that electronic commerce initiatives in Australia could bring about a 2.7 per cent increase in the level of national output, and enhance consumption by about $10 billion within the next decade (National Office for the Information Economy 2000).

The Yellow Pages *Business Index Survey* of Australian small and medium-sized enterprises (SMEs) also provides an insight into the state of affairs in this important segment of the private sector. Figures on electronic commerce procurement rose significantly in the four years 2000–03, (from 17 per cent to 45 per cent amongst small businesses, and from 28 per cent to 64 per cent amongst their medium-sized counterparts), although this growth has slowed down in the past year (Yellow Pages 2001, 2002, 2003).

In 2001, 10 per cent of complaints about electronic commerce procurement related to credit card fraud, although this was an issue for small business only. This suggests that in some respects small businesses may incur the same fraud risks that individuals do, whereas their larger corporate counterparts probably tend more to resemble large public sector agencies than either individuals or SMEs where fraud risk is concerned.

Regarding sales, the 2003 report indicated that online selling as a share of total sales activities may have reached a plateau. While there was a significant increase in the proportion of online businesses that reported more than 5 per cent of their total sales orders online between 2001 and 2002 (from 33 to 43 per cent), this figure remained stable at 43 per cent in 2003. The greatest doubt expressed by respondents in relation to electronic commerce in the latest report was the possibility of people hacking into the system, a major concern for 41

per cent of eCommerce oriented businesses, and a minor concern for a further 32 per cent (Yellow Pages 2001, 2002, 2003).

Payment system usage statistics

Another indication of the extent of electronic transactions in Australia is provided by the Australian Payments Clearing Association's payment transaction statistics, presented in Tables 4.1 and 4.2 below.

Table 4.1: Number of payment transactions, Australia, 1994–2003

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Cheques*	3.7	3.9	3.9	3.7	3.7	3.2	3.1	2.7	2.5	2.3
Direct entry credits*	1.6	1.9	1.7	1.8	1.9	2.1	2.3	2.7	2.7	2.9
Direct entry debits*	0.3	0.4	0.4	0.4	0.6	0.8	0 9	1.1	1.2	1.3
ATM withdrawals**	40.7	38.8	41.6	39.2	42.9	41.9	48.4	64.0	65.4	62.9
EFTPOS**	20.6	29.1	35.5	39.2	44.5	48.6	52.0	57.5	69.4	72.5
Credit cards**	19.9	22.6	24.6	25.9	32.4	42.9	61.9	67.8	84.1	85.6

Note: * millions of items per day
** millions of items per month
Source: Australian Payments Clearing Association 2003, *Payment System Statistics.*

Table 4.2: Value of payment transactions, Australia 1994–2003

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Cheques*	24.8	23.4	24.3	24.9	14.6	12.3	9.7	8.3	7.6	7.2
Direct entry credits*	1.9	2.6	4.2	3.4	3.6	4.9	6.5	9.1	10.3	11.2
Direct entry debits*	1.3	1.2	1.6	1.6	2.4	3.7	5.0	7.0	8.1	8.6
ATM Withdrawals**	4.4	4.9	5.6	5.4	6.2	6.8	7.3	9.4	11.0	11.1
EFTPOS**	1.1	1.5	1.9	2.1	2.4	2.8	3.1	3.5	4.3	3.9
Credit cards**	1.8	2.0	2.3	2.5	3.6	4.3	7.0	8.0	11.2	11.7

Note: * $ billions per day
** $ billions per month
Source: Australian Payments Clearing Association 2003, *Payment System Statistics.*

Although other payment mechanisms are becoming more prevalent, cash is still the most widely used form of payment in retail settings and its use appears to be just as widespread in the 21st Century as it was in the 1980s.

However, a further indication of the extent to which online payments are used is also available by examining the volume of transactions conducted through private sector electronic payment systems. Although most data are commercial-in-confidence, a representative of BPay indicated that for the month of August 2002, approximately eight million electronic payments were made using its services, worth approximately $4 billion.[80] In a survey of 600 main household bill payers conducted in September 2002, it was found that over 50 per cent of

80 Personal communication between Mr Stuart Candy, former Research Assistant to the Committee in 2002 and Mr Andrew Arnott, General Manager, BPay, 1 October 2002.

main household bills were paid using electronic payment methods (including BPay, credit card payments via the phone or Internet, or direct debit), compared with just 15 per cent in 1997 (BPay 2003).

Electronic payment transactions that make use of PIN authentication are governed in many countries by detailed codes of conduct that specify who is liable for loss in certain circumstances, and how payment systems should be used. In Australia, the Electronic Funds Transfer Code of Conduct has been in place for a number of years. Originally this code covered only ATM and EFTPOS transactions, but in April 2002 it was expanded to include all forms of electronic funds transfers, including Internet, mobile phone and telephone banking. This is a voluntary code, but parties who sign the code are bound by its provisions. Compliance with the code is monitored annually by the Australian Securities and Investments Commission.

Over recent years, there has been an increase in the number of complaints made under the Electronic Funds Transfer Code of Conduct, from 42 per million transactions in 1998–99 to 81 complaints per million in 2000–2001. This number remained stable in 2001–2002, with 132,517 complaints being lodged out of approximately 1,640 million transactions. This represents a very small proportion indeed, some 0.008 per cent. On this measure at least, it seems that electronic funds transfer systems operate in a secure and efficient manner (Australian Securities and Investments Commission 2000b, 2002b, 2003b).

Risks for government

As a consequence of the extensive use they make of computers, governments have been frequent targets for new forms of electronic fraud. As government agencies continue to make use of information technologies, so will the opportunities for fraud increase, with potentially profound consequences.

Some recent examples of fraud perpetrated against government agencies from around Australia are described below. Although they extend beyond Victoria, they are indicative of the risks faced by the public sector generally.

Procurement fraud

There are considerable savings to be made by organisations carrying out purchasing and procurement activities electronically. Tenders can be widely disseminated and documents downloaded electronically, while contracts can be negotiated and settled more quickly and easily than in pre-electronic times. This should lead to higher levels of openness, trust and co-operation between those involved in the procurement process (Department of Public Works and Services, NSW 1999). Electronic procurement, however, carries risks of fraud and abuse as internal controls may be removed when new electronic procurement systems are introduced. Government agencies are particularly vulnerable in view of the extensive procurement activities in which they engage and the large sums of money involved. In one Australian case, for example, a

sub-contractor to a local Council in New South Wales allegedly gained access to the Council's database of tendering information and was able to secure numerous contracts through the use of this information (Bell 2000, p.31).

The Victorian Government's 'Electronic Commerce for Procurement' (EC4P) project is intended to streamline government purchasing and tender selection, which accounts for about 12 per cent of all activity in the Victorian economy (Minister for Finance, Victoria 2001). EC4P involves ordering goods and services online from suppliers' electronic catalogues, to be applied across nine government departments (and Victoria Police). Five departments had commenced implementation by 30 June 2002, with a full rollout expected to take an additional two to three years. Projected benefits include fewer steps and reduced paperwork in making purchases, with transaction costs accordingly lower. The priority area of operation has been high-volume, low-value transactions, such as those for stationery, with others to follow (Department of Treasury and Finance 2002). Larger-value purchases are still required to follow the quotation and tendering processes set out by the Victorian Government Purchasing Board (2001).

Electronic ticketing fraud

In New South Wales, the Independent Commission Against Corruption (ICAC) investigated a case in which a number of state government employees of Sydney Ferries at Manly Wharf manipulated the electronic ticketing system to steal approximately $204,000 between 1 July 1994 and 28 February 1997. Ticket sellers discovered that tickets which had been rejected by the ticketing machines for various reasons could still be used by customers to gain access to the ferries. The ticket sellers manipulated the computers to create 4,390 reject tickets which they then sold to customers as legitimate or which they used to claim refunds for themselves. Because the tickets had been rejected, the money obtained did not have to be included in the daily takings for reconciliation purposes.

The corrupt conduct was able to take place principally because management did not fully understand the operation of the computerised system and was thus unable to detect the dishonest conduct. Although the Commission found that five employees had acted corruptly, it did not recommend that any prosecutions take place in view of evidentiary problems associated with proving what had occurred (New South Wales Independent Commission Against Corruption 1999).

Electronic social security fraud

As government benefit programs continue to be administered electronically, the opportunities for electronic social security fraud are also enhanced. Fraud risks have arisen, for example, in connection with Centrelink's Electronic Benefits Transfer (EBT) system that was introduced in 1997 and which now operates nationally to deliver limited social security benefits replacing the traditional counter cheque. Operated with a PIN, the genuine Centrelink client is issued

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

Revenue fraud

Fraud directed at public revenue can also be facilitated through the use of online service delivery. One incident involved the Australian Taxation Office's web site, GST Assist (established following the introduction of Australia's new taxation system), being compromised. A student known variously by the aliases K2 and Kelly exposed a glaring security breach in the web site. Simply by typing in a string of numbers, K2 was able to gain access to the records of more than 20,000 GST-registered providers, which contained their bank account details. He alerted more than 17,000 of the providers by sending their confidential details to them by email (Dancer 2000, p.76).

In May 2003, following the execution of 58 search warrants across the Sydney metropolitan area by the Australian Federal Police, six arrests were made of people allegedly implicated in a major taxation fraud involving the production of approximately 170 fraudulent income tax returns. Requested refunds totalled $2.1 million, of which $1.5 million has been paid out (Australian Federal Police 2003, p.77).

Electronic money laundering

Another area of concern relates to electronic money laundering. The growing application of telecommunications technology to the banking industry has provided new means of money laundering. Electronic funds transfer methods can greatly facilitate layering (or moving assets in a series of transactions to conceal their identity), and thus more effectively obscure the money trail. So too can the process of integrating funds into the mainstream economy be facilitated by electronic transfers: dirty funds deposited with a complicit financial institution can be used as collateral for a loan, speedily recovered and invested in a legitimate business.

In one alleged money laundering operation based in the Netherlands, sexually explicit Internet sites were used to launder the proceeds of drug trafficking by transferring funds to a number of accomplices who used them to purchase services from an Internet site conducted by the drug trafficker. Because the money appeared to have been legitimately earned by the web site operator, its illegal origins were disguised. A prosecution failed because of insufficient evidence relating to the illegal source of the funds.

In one recent case, an individual in Victoria was involved in laundering a total of $39.9 million in 'black cash' obtained from merchants between 1990 and 1997, resulting in the Australian Taxation Office being defrauded of some $20 million. The principal offender received a commission of between 2 and 6 per cent of the money so laundered, which amounted to approximately $800,000. The technique used by the offender was to pay the money into an account opened in the name of a fictitious charitable organisation so that the money could be transferred to overseas accounts. The charitable organisation account was an internal bank management account that was unlikely to attract the attention of the regulatory authorities. The account was opened using false names and the funds transfer instructions given also used false names. The principal offender was sentenced to imprisonment for seven years with a non-parole period of four years and six months (as increased following an appeal by the Commonwealth *DPP* v *Goldberg* [2001] VSCA 107, Court of Appeal, Supreme Court of Victoria, 27 July 2001).

Smart cards may also be used for money laundering purposes, particularly if value can be transferred from card to card without the involvement of a financial institution. It is also considerably easier to transport a fully loaded stored value card across an international boundary than it is a suitcase full of cash.

Insider trading

In one New South Wales case investigated by the Australian Securities and Investments Commission, a former merchant banker was convicted of insider trading charges that related to him acquiring 5,000 $2 call options in a company in September 1996, when he had knowledge that the company was likely to be the subject of a takeover bid. He had withdrawn cash and purchased the options in the false name of 'Mark Booth' and paid for them with nine cheques for separate amounts, each under the reporting threshold of $10,000 and totalling approximately $90,000. The offender acquired a profit of $2 million, which was subsequently returned to the people who had sold the call options. He was found guilty of offences under the Corporations Law and the *Financial Transaction Reports Act 1988* (Cth) and sentenced to two years and six months' imprisonment with a non-parole period of one year and eight months. He was also fined $100,000 (R. v *Hannes* [2002] NSWSC 1182, Supreme Court of New South Wales, 13 December 2002). Cases such as this are clearly facilitated through the use of electronic trading systems and the ability to fabricate documents electronically.

Electronic funds transfer fraud

In one case of electronic funds transfer fraud a financial consultant formerly contracted to the Department of Finance and Administration was convicted on 25 September 2001 of defrauding the Australian government by transferring $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 seven years and six months' imprisonment with a non-parole period of three years and six months (R. v *Muir*, Supreme Court of the ACT, 25 September 2001). Two other individuals who were alleged to have been involved in this fraud were acquitted in the ACT Supreme Court on 11 September 2003 (Campbell 2003).

Health benefits fraud

In Australia, the Health Insurance Commission (HIC) processes claims and makes payments for the provision of health services and other benefits under various government programs. Many transactions are now conducted electronically, which creates substantial risks of misappropriation of funds and fraud by reason of the large sums of money involved. Although the most common offences investigated by the HIC relate to health care providers or members of the public making false claims for Medicare or pharmaceutical benefits, opportunities also arise for employees of the Commission itself to manipulate the electronic claims processing systems. Risks include electronic claim forms being counterfeited or manipulated, digital signatures being compromised, and electronic funds transfers being altered or diverted away from legitimate recipients (Smith 1999). 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 1998).

Fraud can also be committed by members of the public, health care providers or practice staff. In June 2000, the Australian Federal Police began a joint investigation with the HIC into false Medicare claims valued at approximately $109,000 being submitted by medical practice receptionists. In May 2002 a woman was convicted of defrauding the Commonwealth and theft, and sentenced to three years and six months' imprisonment with a non-parole period of 15 months. Two others were convicted and sentenced to suspended terms of imprisonment and four others pleaded guilty to various offences (Australian Federal Police 2002, p.39).

In another case, between April and December 1995 an offender wrote out applications for birth and death certificates of various people who had generally died at a very young age a number of years ago. In most instances the certificates were supplied by the Registry of Births, Deaths and Marriages in Sydney. The offender obtained birth and death certificates in false names and forged

Medicare application forms in false names and submitted them to the HIC. He also attempted to open, in one case, and actually opened, in the other, bank accounts in false names, into which he deposited the proceeds of his fraudulent claims. He was convicted of various state and federal offences and sentenced to a term of imprisonment of four years with a non-parole period of 18 months (R. v *Knight* [2001] NSWCCA 114, New South Wales Court of Criminal Appeal, 30 March 2001).

The HIC's 2000/2001 annual report indicates that Victoria stands below the current national average on the HIC's scale for measuring suspected Medicare benefit abuse (Health Insurance Commission 2001a).

Credit card fraud

Fraud relating to government credit cards is also a risk. The Australian Civil Aviation Safety Authority identified two cases in which its officers abused travel cards issued for official business. One individual withdrew his travel allowance from the Authority's bank and then used his travel card to pay for accommodation, meals, drinks, and in-house videos while on official business. Another officer used the travel card as a form of personal credit line by withdrawing cash and repaying it later at his convenience (Joyce 1999). Although most cases relate to government cards being used by authorised users for unauthorised purposes, the possibility of credit cards being stolen or counterfeited also exists.

Theft of information

Electronic fraud may also arise where information is stolen from electronic databases, although arguably this goes beyond the concept of fraud in the strictest sense of deception. Theft of information, a form of electronic theft that overlaps with electronic fraud, could also entail the infringement of various laws including laws relating to intellectual property, privacy and the criminal law. Often it is not the theft of information that is of greatest importance but the use to which that information is put.

In one case, for example, charges were laid against an employee of the Australian Department of Social Security (DSS) following the removal of a large number of records from the Department's database. Details of individuals held on the database were sold to a private investigator who sold them on to insurance companies (Australian Federal Police 1996). In 1996 an employee of the DSS, who was a former police detective, was sentenced to 200 hours' community service and fined $750 in Sydney after he was found guilty of unlawfully gaining access to and disclosing DSS information (Australian Federal Police 1997).

Computers have also been used for economic espionage. Some years ago, the New South Wales Independent Commission Against Corruption investigated employees of the national telecommunications carrier, Telecom (as it then was), who had sold confidential government information to private

investigators (New South Wales Independent Commission Against Corruption 1992).

Another example of theft of information is a case in which credit card details from over 8,000 customers of Melbourne's CityLink tollway database were allegedly used by two Victorians to purchase up to $80,000 worth of goods and services. It was reported that the two men also sold some of these goods on Internet auction sites but failed to deliver to the winning bidders. The credit card details are alleged to have been used to fund travel expenses during an extended break interstate last year, although the accused were not arrested until returning to Colac, in western Victoria, to visit the family of one of them. In this case, credit card information was said to have been provided by a former employee on a floppy disk rather than through hacking an online database (Australian Associated Press 2002a, 2002b).

Theft of computer hardware and software

Definitional issues also arise regarding the theft of computer hardware, as this would generally not involve fraud but rather conduct that may be a precursor to the commission of crimes of dishonesty. Government employees, for example, could steal computer equipment that may contain valuable software and perhaps sensitive information that could be used for other criminal activities. In one recent investigation undertaken by the Australian Federal Police, a government department was the victim of a series of thefts of computers containing sensitive information. A number were recovered and three individuals were charged. The department has since undertaken a review of its security and employee screening procedures to prevent the occurrence of similar incidents (Australian Federal Police 1999).

More recently, two computer servers belonging to the Australian Customs Service (ACS) that contained confidential access codes and passwords were allegedly stolen from Sydney International Airport by former ACS employees apparently acting out of revenge following a dispute over employment. New passwords were issued prior to any confidential data being accessed (Walker 2003).

Inappropriate use of information technologies

Finally, public sector employees may misuse information technologies provided at work by using them for their own unauthorised purposes. Despite clear warnings of the consequences of inappropriate use of the Internet in the workplace, cases continue to emerge of staff misusing the Internet in this way. In a number of widely reported cases, employees have been disciplined or dismissed for using workplace computers inappropriately. In New Zealand, for example, four employees of the Department of Child, Youth and Family Services were dismissed for inappropriate use of the Internet that included gaining access to pornographic material (The *Age*, 11 July 2000, p.2).

Although it might not be possible to describe such conduct as fraudulent, it can result in considerable loss of productivity as well as creating an unprofessional

culture in the workplace and potentially leading to problems of legal liability. An employee may be defrauding the government simply through failing to work appropriate hours.

Risks for business

Plastic card fraud

In most cases of online fraud involving consumer purchases, it is the merchant rather than the consumer that suffers the loss. Where an offender has ordered goods or services using someone else's credit card, and where the cardholder has not contributed to the commission of the offence, the financial institution will 'charge-back' the amount debited to the cardholder's account to the merchant who must then take remedial action against the offender – which is rarely possible.

One recent case of abuse involved credit card information that was disclosed in an unencrypted email message from a New Zealand consumer who purchased a book from an online book vendor. The woman purchased the book with her debit card and gave her mobile phone number as a contact number.

The book arrived, but a few days later she found her debit card had been used to make a number of unauthorised purchases from companies in Portugal, Indonesia and Brazil. All of the charges included the information she had given only to the vendor – her card number, address and mobile phone number. She also discovered that five new accounts had been opened with her details (Slane 2001). In such cases the consumer is unlikely to be liable for the unauthorised purchases.

Merchants can also be defrauded in relation to the payment systems that they use. In Victoria, the Major Fraud Investigation Division has investigated numerous incidents relating to identity fraud. One investigation focused on a young male offender who stole three EFTPOS terminals from three separate merchants. With the EFTPOS terminals the offender was able to take over the identity of each merchant and undertake refunds and transactions against the merchants' accounts to the value of $20,000 (Victoria Police 2002).

Card skimming

One of the most recent fraud concerns to emerge in the financial services industry is card skimming, or the illegal capture of information from a plastic payment card's magnetic stripe, used in conjunction with the card's illegally obtained PIN authorisation numbers. The information from the card can be skimmed in a few seconds by passing the card over a reader either hand-held or fixed to an ATM or other suitable location where unsuspecting users will believe that the device is being used legitimately. Micro cameras or telephoto lenses on cameras are then used to record the user's PIN. Equipped with the account information and PIN, the offender can then create a counterfeit card and use

the PIN to withdraw funds from the account. It was noted in one submission to the Committee that emerging technology has enabled the process of skimming to become more covert, with some skimming devices being as small as a pager or matchbox.[81] It is now easy for a criminal posing as a waiter or retail assistant to swipe a card without the cardholder being aware, or to attach a skimmer to a bank's ATM, which records the cards magnetic stripe data.

Counterfeit cards are a growing problem for Victorian law enforcement agencies, with crime syndicates from Asia and Europe now targeting Australia as a country to make transactions using the counterfeit cards, often created through card skimming. It is common practice for counterfeit cards to be imported into Australia by these organisations. However, importation is not the only means by which cards are obtained. Recent police operations have also uncovered small-scale credit card factories in Australia where credit cards are being manufactured.[82]

In one recent case, for example, a Malaysian national who had entered Australia on a tourist visa, Kok Meng Ng, pleaded guilty to four offences under the *Financial Transaction Reports Act 1988* (Cth). He admitted to stealing $623,426.91 from 315 Commonwealth, St George and Westpac Bank customers after having skimmed their cards at 36 ATMs around Sydney between May 2001 and November 2002. He then made 64 transactions over 18 months, depositing about $200,000 in bank accounts held by the Hong Kong and Shanghai Banking Corporation in sums of less than $10,000 to prevent the transactions being detected by AUSTRAC. He was sentenced to three years' imprisonment at the New South Wales District Court on 30 October 2003 (Australian Associated Press 2003; Barker 2003a).

A number of submissions received by the Committee noted the prevalence of this type of activity throughout Australia, much of it involving organised crime groups from other countries.[83] It was noted in one submission to the Committee that although much card skimming was seen to be led from overseas, skimming is now also becoming a domestic activity and merchants are seriously concerned about the impact that this may have on their business/brand reputation.[84]

81 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

82 Ibid.

83 Mr Jilluck Wong, Regional Director, Fraud Prevention, American Express, in conversation with the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, Sydney, 25 June 2003; Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003; Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, Sydney, 1 October 2003.

84 Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

Theft of personal information

A related risk concerns the theft of personal information from databases, which can then be used to commit fraud. Organisations that engage in electronic transactions maintain extensive databases of personal information. These include names, addresses, bank account details, credit card details and perhaps also detailed personal information relating to patterns of purchasing, which can be used for marketing purposes. Considerable opportunities arise for criminals when such information is not held securely, not only for misusing identities, but also for targeting victims more easily and extensively. The CityLink case cited above is an important example of this, as it had implications not only for the Victorian government but also for TransUrban, the private owner and operator of the CityLink electronic tolling system.

Online funds transfer fraud

The Internet may also be used in connection with the commission of various forms of theft of funds electronically (see Grabosky, Smith & Dempsey 2001). Sometimes security information such as passwords and account details can be obtained by gaining access to databases held by businesses or financial institutions. On other occasions insiders may move funds electronically by sending instructions via electronic mail. When the use of electronic commerce becomes more widespread, abuses relating to the transfer of funds electronically can be expected to increase.

In giving evidence to the Committee, a representative of the Corporate Crime Liaison Group referred to a case in which a customer sent regular periodic payments by electronic funds transfer to the supplier of goods on a fortnightly basis. One such payment was to be in excess of four million dollars. Prior to authorising the transfer, the customer received a letter ostensibly from the supplier, saying that the details of the supplier's bank account had changed and that the funds should be remitted to a new account, details of which were provided. The customer did not question the information given as it was provided on a legitimate-looking letter. The funds were then transferred into the specified account that was with the same bank and branch as the legitimate account of the supplier. It transpired that the funds had been transferred to an account opened by the offenders for the purpose of defrauding the customer. The offenders had downloaded a logo from the supplier's web site and used it to fabricate the dishonest letter of instructions given to the customer. Following the completion of the transfer, the offenders managed to withdraw some of the funds from the account prior to the fraud being detected. As electronic funds transfers are being used more often and for larger sums, Mr Dean Newlan of the Corporate Crime Liaison Group considers this type of dishonest practice to be a high area of risk for the future.[85]

85 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

Page jacking

Page jacking involves the appropriation of web site descriptions, key words, or meta-tags from other sites. Page-jackers insert these items into their own sites in an attempt to draw individuals to a particular site. The victim is then defrauded in various ways, sometimes by having modem connections re-directed to international premium paid numbers.

One such case involved a company which advertised 'free' erotic photographs on the Internet. In order to see the images, the user was required to download software which, once installed, took control of the user's modem, cut off the local ISP, and dialled a number in the former Soviet Republic of Moldova in Eastern Europe. The line remained open until the computer was turned off resulting in the user incurring large international telephone charges that were shared between the offender and the Moldovan telecommunications company. The fraud was detected through regular surveillance of customers' telephone accounts and the United States Federal Trade Commission was able to obtain an order requiring the defendants to place US$1 million in an escrow account pending resolution of the case (*Federal Trade Commission* v *Audiotex Connection Inc.* Eastern District of New York, filed 13 February 1997).

Users' browsers can also be manipulated so that attempts to close the browser's windows or to use the 'back' or 'forward' button will simply direct the user to another site controlled by the offender (Department of Justice, United States 1999).

Outsourcing risks

Various economic crime risks also exist in connection with the outsourcing of services, particularly those relating to information technology and data management (Bell 2000). The use of Application Service Providers (ASPs) that provide storage space for digital information belonging to other entities on a commercial basis creates risks that the information may be used for fraudulent purposes or sold on without authority. The outsourcing of information technology services generally also creates risks of fraud and corruption where contractors abuse the trust that they are given in managing confidential and sensitive data.

Digital extortion

The Internet is also being used to carry out acts of criminal extortion. These acts may not qualify under a strict definition of Internet fraud but they warrant attention here because they can have substantial consequences for individual businesses. In one case, two individuals from Kazakhstan were arrested in London on 20 August 2000 for allegedly having broken into the computer network of Bloomberg LP, Manhattan, in an attempt to extort money from the company. The arrest was made following a joint operation between the FBI's New York Field Office, the Metropolitan Police in London and authorities in Kazakhstan (Federal Bureau of Investigation, United States 2000).

One Australian case involved a 27-year-old male, known as 'Optik Surfer', who was sentenced on 27 March 1998 in Sydney to three years' imprisonment (with 18 months suspended) for eight counts of obtaining unlawful access to a computer, and one count of unlawfully inserting data into a computer.

The offender, who was a computer networking consultant, had been refused employment with an ISP in January 1994, and in March 1994 took revenge by illegally obtaining access to the company's computer network using the user account and password of the company's technical director. He then gained access to the company's database of 1,225 subscribers and publicised their credit card account to various journalists. He also altered the company's home page on 17 April 1994, including a message that the company's security system had been compromised. The publicity resulted in the company losing more than $2 million in lost clients and contracts. It was required to change its business name and sold the Internet access part of its business to another ISP (R. v *Stevens,* District Court of New South Wales, 27 March 1998; appeal to the New South Wales Court of Criminal Appeal dismissed on 15 April 1999 [1999] NSWCCA 69).

Theft of services

As with other types of telecommunications, it is possible to steal Internet-related services by entering into a contract with an ISP and a telecommunications carrier, and then failing to pay for the services provided. Fraud of this nature may be committed against service providers by both individual consumers and business entities. One submission to the Committee noted an increase in this type of fraud, particularly concerning false establishment and manipulation or misuse of mobile telephone accounts.[86] On occasions, insiders within telecommunications companies may be involved in dishonest activities. Employees could, for example, make use of other people's passwords to gain access to networks to commit fraud. In July 2003, it was reported that two Melbourne employees of Telstra were alleged to have used stolen SIM cards to incur mobile phone charges in other people's names (Sexton 2003).

A related problem arises where a person visits a web site that manipulates the telephone billing system and results in large international calls being billed, as in the Moldovan scam referred to above. Sometimes the telecommunications carrier will agree to provide compensation where the customer has acted innocently.

86 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

Risks for individuals

Identity-related fraud

One of the most common strategies used to perpetrate fraud, as already noted, is the creation and use of false documents for misrepresenting 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 (Smith 1999; see also 'Fraud in the corporate and business sector', Chapter 2).

The problem of identity-related crime is particularly acute in cyberspace, where, as the famous cartoon in the *New Yorker* observed, 'on the Internet, nobody knows you're a dog'! (July 1993, p.61).

Online 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 email by stripping them of identifying information and allocating an anonymous identifier, sometime encrypted for added security. By using several re-mailing services, users can make their communications almost impossible to trace.

Anonymity can also be achieved in cyberspace using less technologically complex means. Simply purchasing a pre-paid Internet access service from an ISP and renting a telephone line from a carrier, each in a false name, provides an easy means of achieving anonymity. Free email services offered by some ISPs are 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 the user's 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 checks undertaken when such services are obtained.

Even electronic commerce technologies that make use of public key infrastructures and digital signatures can be manipulated. Individuals can present fabricated documents to support a false identity when registering with a Registration Authority 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 online 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 email and Internet Relay Chat that provide higher levels of anonymity were found to be preferred by those engaging in online 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.

An illustration of the use of strong 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, 1,300 videos and 3,400 floppy disks. One member of the Club co-operated with police and this led to approximately 100 arrests around the world in September 1998 (Australasian Centre for Policing Research 2000, p.126).

Local forms of computer crime may also involve anonymous activities. The case of R. v *Muir* (Supreme Court of the ACT, 25 September 2001, discussed above), is a prime example of this. The common feature in these cases is that the offenders use other people's identities in verbal representations, through false identity documents or the misuse of passwords.

Misleading domain names

As is the case with the registration of misleading business names and misuse of trade makes and brand names, difficulties have arisen with the registration and use of domain names. In the absence of a global system of registration, it is possible to choose domain names that closely resemble well known companies in order to trick consumers into entering into contractual arrangements with a dishonest individual.

It is possible to choose legitimate-sounding names in order to improve one's credibility or to include domain names which are misleading (see Bachner & Jiang 2000). An example is the recent development of a practice by some organisations in the United States and Canada of 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.

An attempt was made in 2000 to duplicate the web site of leading online payment service PayPal, under the very similar URL http://www.paypai.com (using the letter 'i' instead of 'I'), so as to capture unwitting users' personal information (Sorkin 2001).

There is also no failsafe way of ascertaining the bona fides of claimed commercial affiliations on the Internet. Referees for organisations might be individuals employed specifically to indicate their approval of the organisation in question.

Web page mirroring

A related problem concerns mirror web sites which are created by offenders to deceive consumers into disclosing credit card details when making purchases.

In New South Wales, such a case has been investigated in which the offenders copied official web sites of premier entertainment venues to almost every detail, including theatre layouts and restaurant information. Programs were constantly updated to maintain the facade of legitimacy. The crucial difference was that the copy site had its own credit card booking arrangement, so that customers' money would be credited to the offender's account. The bogus site for Sydney appeared on the Internet with a similar URL to the genuine site. The offenders have created 23 similar sites mirroring opera houses in Europe, including Paris and Vienna. The computer crime unit of the New South Wales Police Commercial Crime Agency contacted the FBI after tracing the bogus site to a Miami Internet server. Since then, the server has re-located to California (Kennedy 2002).

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).

Investment scams

Most frauds involving business transactions carried out on the Internet mirror activities conducted using traditional paper-based techniques. On the Internet, however, criminals now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost. Examples include so-called advance fee schemes, such as pyramid and Ponzi schemes, the use of chain letters and bulk electronic mail, business opportunity schemes, and fraudulent online auctions, prizes and lotteries. Even the endemic West African advance fee letter scams are now being conducted using email, as the true identity of the sender is easy to disguise and original supporting documentation is unable to be checked for authenticity (Smith, Holmes & Kaufmann 1999).

Marketing scams

Other frauds carried out through the Internet involve the non-delivery of goods and services or the delivery of defective products and services. Particularly prevalent in business contexts are scams involving computer products and services and financial services, while in the realm of consumer transactions, health and medical products, and the provision of sexual services, have often been found to be dishonest.

International Internet Sweep Day, a co-operative effort undertaken by consumer protection agencies around the world, was launched in 1997. In that first year, during the 24-hour sweep, more than 1,100 sites advertising suspicious get-rich-quick schemes were located (see 'Internet sweeps' in Chapter 8).

Finally, the Internet is being used for various forms of unsolicited or bait advertising and illegal inertia selling techniques infringing local consumer

protection legislation.[87] Although many of these scams seek to defraud consumers, they can just as easily target businesses and government agencies.

Internet gambling

One expanding area of risk lies in the growing industry of online gambling services. Although a number of legitimate providers of such services exist, there are many ways in which unscrupulous operators can take advantage of some of the most vulnerable users of the World Wide Web. The odds of winning some casino-style games might be unduly weighted against gamers, identification details registered with the operator by prospective players – including credit card information – might be misused, or winnings may be withheld.

The *Interactive Gambling Act 2001* (Cth), which commenced on 11 July 2001, followed a year-long moratorium on the establishment of new Internet gambling sites. The Act prohibits the provision of certain Internet gambling services including online casino gaming to customers in Australia. Apart from certain exceptions such as microwagering and instant lotteries, the prohibition does not extend to online versions of wagering, sports betting or lotteries (Nettleton 2002). The rationale for the prohibition is explained in the Second Reading Speech on the Bill:

> The Government is concerned that the increased accessibility of gambling services via communications technologies such as the Internet has the potential to significantly exacerbate problem gambling among Australians (Parliamentary Debates, Australia 5 April 2001).

Even where these services are provided under careful scrutiny to ensure their integrity, as in the closely regulated offline gaming sector in Australia, it is seen as inevitable that increased access will be accompanied by an increase in gambling-related problems.

Under Part 3 of the Act, the Australian Broadcasting Authority (ABA) is the body responsible for making and investigating complaints about prohibited Internet gambling content. Between 11 January and 30 June 2002, only 10 such complaints were received (Australian Broadcasting Authority 2002). Of these complaints, two were terminated due to a lack of sufficient information, when no prohibited content could be found at the sites provided. A further six related to sites located outside Australia. In these cases, the ABA notified the makers of filter software products about the content of the sites, as required by the Interactive Gambling Industry Code of Conduct (Internet Industry Association 2001). While the remaining two investigations related to Australian-based sites, the ABA determined that the matters did not warrant referral to the Australian Federal Police for prosecution (Australian Broadcasting Authority 2002).

The basis for the current arrangements is expressed in the Code as follows:

87 Inertia selling involves selling or sending unordered goods to consumers and billing them in the hope that they will accept the goods and pay the bill without question.

> In relation to the prevention of access to prohibited Internet gambling content, supervision by responsible adults remains the effective means of protection, particularly in the case of Internet use by children (Internet Industry Association 2001, p.3).

The problem, however, relates to cases in which adults themselves use prohibited Internet gambling services.

Although the scale of the problem appears to be minimal, the nature of the regulatory approach is such that compliance is left to the end user, and there is no means of ensuring that online gambling is not occurring. Those Victorians determined to gamble online, whether due to curiosity or to gambling addiction, may do so simply by deciding not to use the ISP-provided filtering software.

In the United States, it has been argued that laws prohibiting online gambling have done little to stem the flow of dollars from the United States to offshore gaming sites. According to recent estimates, residents in the United States currently provide about half of all money spent at gambling sites worldwide (Glasner 2002).

The legislation, with its substantial fines, may be effective in preventing the provision of certain online gaming services to Australians by local providers. However, it seems likely that Victorians who want to gamble online will do so, but without the protection that could be made available through using a trusted, regulated local operator. Any fraud that takes place is therefore almost certain to be perpetrated by overseas individuals or businesses, giving rise to the usual problems entailed in international prosecution and law enforcement. Licensing and regulation of gaming providers, as envisaged by the *Interactive Gaming (Player Protection) Act 1999* (Vic) which would apply to local Internet casino providers in the absence of the federal prohibition, coupled with extensive public education and awareness-raising efforts may eventually prove to be a necessary alternative to the current approach.

Online auctions

The development of online auctions, which has been highly successful globally, has also created many risks for consumers and businesses alike. A report of the Internet Fraud Complaint Center (IFCC) in the United States estimated the daily number of transactions to be 1.3 million in 2001. Unfortunately, Internet auctions account for a very high proportion of instances of online fraud. The IFCC found that 64 per cent of all reports it received were related to auction fraud. A market research company, eMarketer, found an even higher rate (87%) of cases of online auction fraud in 2000 (Internet Fraud Complaint Center 2001b).

The world's largest online auction house, eBay, claims to have some 50 million registered users worldwide (Wolverton & Gilbert 2002) and reports a fraud rate below 0.1 per cent. However, this figure includes only cases that are reported to eBay and come within its own definition of fraud.

There are several ways in which online auction fraud may occur (Internet Fraud Complaint Center 2001b). Dishonest purchasers may make use of another person's bank account information (a straightforward case of 'identity theft'), or engage in multiple bidding (inflating the price using aliases, then withdrawing the higher ones at the last moment to secure a lower price). Dishonest merchants may misrepresent the item's value, or engage in fee stacking (in which extra expenses are added after the auction is over), or employ shill bidding (where the seller drives up the price of his or her item with false bids). Since customarily payment is required before delivery, non-delivery of an (often non-existent) item purchased at auction and paid for is the most common form of deceit. 'Triangulation' is a complex fraud involving the fraudster purchasing an item using stolen payment details, then selling it on to an innocent buyer, thereby retaining the cash and transferring the risk of seizure to the end recipient.

It should be noted that the risks are not equal for every transaction. An individual buyer need not be exceptionally astute to assess the risk involved in a seller defaulting prior to completing the transaction. Moreover, whether the risk of fraud is borne ultimately by the buyer, the seller or a third party (most likely the online auction house or a financial service provider) depends on the payment method used and various other arrangements specific to the case at hand (Sorkin 2001).

Consumer education is perhaps the most effective way of preventing the occurrence of what is clearly one of the most prevalent kinds of fraud affecting individuals online.

Prepaid mobile services

A similar issue to 'Smart card fraud' (discussed above) arises in relation to prepaid mobile telephone services and card-accessed services, such as the now ubiquitous international calling cards. However, here the risk is for individual consumers rather than businesses.

Both prepaid mobile services and calling cards involve the customer's credit being centrally stored, with card access provided by a PIN. Charges per minute vary according to the country contacted, and with a range of surcharges and connection fees the formula can become complex. Since rates are controlled centrally by the service provider, these may be altered from the tariff advertised without notice, and any charging 'errors' are borne by the customer, who may not even detect them but whose purchase monies have long since been processed. With calling cards, the widespread policy of charging for every minute or part thereof also weighs the transaction in favour of the service

provider. With myriad small providers in this sector of the telecommunications industry, this system may be vulnerable to fraud.

This type of fraud, which involves the accumulation of many inconsequential amounts to generate a larger sum for the service provider, might not readily be detected and reported, as generally individual customers would suffer very small losses. It may also be associated with particularly complex evidentiary issues.

Online banking

The large increase in remote delivery channels for financial services such as telephone banking and online banking means that face-to-face contact between financial institutions and their customers is becoming less frequent and in some cases may never occur. The use of intermediaries such as financial brokers, loan introducers, third party agents, and outsourcing initiatives presents new challenges in controlling fraud (see Chapman & Smith 2001). Each of these areas poses risks for consumers as well as for providers of financial services.

Recently Australian and overseas banks have been victimised by individuals sending spam email messages asking the recipients to click on a link to re-activate their online banking facilities. The message purports to come from the customer's bank but the link takes the user to an illegitimate web site that is used to capture the username and password of the customer. This can then be used for illegitimate online banking purposes. In March 2003, the Australian Federal Police responded to the unauthorised mirroring of the Commonwealth Bank Internet banking web site. The suspect(s) constructed a false web site purporting to be the legitimate Internet banking site. Emails were sent to customers directing them to the web site and requiring them to access the site and enter their account numbers and password; the reason given was an upgrade in security. The suspect(s) captured the usernames and passwords that were then used to access the accounts of 70 customer bank accounts. Funds from 12 customers were then transferred to an account belonging to a Sydney-based person. This person was arrested by New South Wales Police and the Australian Federal Police in a Sydney bank in mid-March 2003 while attempting to withdraw the siphoned monies (Australian Federal Police 2003, p.75). Recent investigations by the Australian High Tech Crime Centre in conjunction with the Federal Bureau of Investigation in the United States have led to one of the illegitimate sites allegedly based in Florida being closed down (Barker 2003b).

Non-provision of services

Consumers may suffer loss where ISPs fail to deliver the services they agree to provide. As online consumers continue to increase their use of the Internet, so the number of complaints about ISPs increases. In Australia, for example, complaints to the regulatory agency, the Australian Competition and Consumer Commission (ACCC), have included allegations of overbilling, inadequate

detail when billing, failure to supply technical support and other services as represented, failure to connect consumers to the Internet as agreed, failure to honour requests to disconnect, disputes concerning the need to have a credit card to obtain services, claims of inadequate recognition of consumers' legal rights, and allegedly false misrepresentations about the speed of Internet access and the experience of the Service Provider (Australian Competition and Consumer Commission 1999). In May 1999, Consumer Affairs Victoria reported on an ISP which had offered unlimited Internet access for 12 months for an up-front fee of $250, but whose services customers had enjoyed for only two to five weeks before being disconnected. By the time complaints were investigated the company's phone lines had been disconnected and its premises vacated (Consumer Affairs Victoria 1999).

Individuals, businesses and government entities can all be victimised in this way. Although such conduct may result in a civil action for breach of contract, the present discussion focuses on criminal consequences, such as prosecution for theft, dishonesty, and other offences involving misleading practices.

Securities and investment fraud

The Internet is now used regularly for corporate activities that extend from offering and trading in securities to lodging official documents electronically with regulatory agencies. Already instances have begun to emerge of fraudulent conduct involving the share market in which the Internet has been used to disseminate false information in order to attract investors or to manipulate share prices.

The accessibility of online share trading facilities has brought about unprecedented opportunities for share market manipulation. The proliferation of day traders contributes to the volatility of share prices, particularly in those securities that are thinly traded. Against this background, structuring transactions so as to give the impression of momentum in the price of a share could be readily accomplished by an individual or investors acting in concert (Grabosky, Smith & Dempsey 2001).

Bulk email programs allow stock promoters to send personalised messages to thousands and even millions of Internet users simultaneously. In the Asia–Pacific region, a number of instances have been discovered of Westerners based in the Philippines, Indonesia and Thailand using high pressure marketing techniques to sell non-existent or over-priced financial products to investors worldwide. In one recent operation, 70 foreigners were arrested in Bangkok for using unsolicited telephone and email contact to promote share investments (Australian Securities and Investments Commission 2001).

In another recent case, a 24-year-old man from a Melbourne suburb manipulated the share price of an American company by posting information on the Internet and sending email messages around the globe that contained false and misleading information about the company (Tomazin 2001). On 8

and 9 May 1999 the man posted messages on Internet bulletin boards in the United States and sent more than four million unsolicited email messages to recipients in the United States, Australia and other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than 10 times the previous month's average.

Several days before he transmitted the information the offender purchased 65,500 shares in the company through a stockbroking firm in Canada. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000. The offender was prosecuted by the Australian Securities and Investments Commission (2001) for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that 21 months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500 (*Australian Securities and Investments Commission* v *Steven George Hourmouzis*, County Court of Victoria, 30 October 2000). In a separate prosecution, Wayne Loughnan of Cawarral in central Queensland, who assisted Hourmouzis in the share market manipulation, was sentenced to two years' imprisonment, wholly suspended, in the County Court of Victoria on 22 May 2001.

Superannuation fraud

Currently in Australia there are over 100,000 superannuation funds. By the year 2020, the superannuation savings pool may rise to some $2,000 billion. Such large sums of money create opportunities for both fraud as well as mismanagement, and already there have been instances of superannuation fund managers defrauding fund holders. (See, for example, the case of R. v *Houghton* ([2000] NSWCCA 62, New South Wales Court of Criminal Appeal, 10 March 2000), in which $1,376,293 was removed from trust funds for investment in speculative endeavours). The large sums of money currently being handled by superannuation funds also create risks of money laundering. Although outside the scope of the present Inquiry, such a practice has definite relevance in terms of the disposal of fraudulently obtained funds.

Conclusion

The development of new technologies has unfortunately, but inevitably, been accompanied by new opportunities for dishonest people to trick and deceive those with whom they communicate and conduct business online. Some of the fraudulent practices outlined above merely reproduce traditional scams, adapted to the electronic environment. Other fraudulent practices use new technologies for novel illegal purposes. The concern for regulators is that often those who commit electronic theft will be located in other places, making detection, investigation, prosecution and punishment more difficult. The following chapter will consider some steps that can be taken to help prevent such theft, and fraud in general, from occurring in the first place.

5. Prevention Policies and Codes of Practice

Introduction

A wide range of strategies has been devised to deal with white-collar crime and fraud. Some of these entail using the traditional legal measures of prosecution and punishment, while others focus on changing attitudes and practices within the workplace in order to prevent illegal conduct from occurring in the first place (Smith 2002b). Although legally-based deterrence will always have a place in controlling fraud and economic crime, the difficulty and expense associated with taking legal proceedings against offenders mean that other organisational measures need to be adopted in the first instance. In this sense, the business and professional communities have much to offer in regulating the conduct of their own members, leaving formal policing and prosecution for the hopefully rare instances in which organisational regulatory controls fail.

The importance of taking steps to prevent fraud was noted by a number of those who gave evidence to the Committee. The Executive Officer of the Australasian Centre for Policing Research, for example, likened the situation to the regulation of illegal drugs, claiming that prevention or minimisation is preferable to remedying the problem after the fact. He saw the solution as being to 'educate the community, educate government, educate business, to make it as hard as we can in the first place'.[88] The Performance Audit Director of the New South Wales Audit Office also saw prevention as being of primary importance 'because detection by itself [is] very expensive, very time consuming and not very effective'.[89] Other evidence to the Committee supported the view that taking fraud detection measures was very costly and therefore less desirable commercially than implementing preventive measures.[90]

---

88 Mr Des Berwick, Executive Officer, Australasian Centre for Policing Research, in conversation with the Committee, 3 October 2003.

89 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

90 Mr Dennis Challinger, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

Representatives from both the Corporate Crime Liaison Group (as it then was) and KPMG also stated that fraud prevention measures were of great importance, advising the Committee that most fraud in the corporate sector is due to a lack of internal controls.[91] For example, Mr Newlan, representing the Corporate Crime Liaison Group, noted that 'in our experience… poor internal control and fraud in the corporate sector go hand in hand. It is rare that you do find a case of fraud where poor internal control is not present.'[92]

In the absence of adequate internal monitoring, even a lone operator can have considerable impact. Nick Leeson, a trader with Barings, Britain's oldest merchant bank, took actions which single-handedly led to the bank's collapse by accumulating £800 million of debt in 1994–95. He had previously enjoyed enormous success and in an effort to buy his way out of the downward turn, found internal flaws in the bank's monitoring system which allowed him to conceal his losing streak from colleagues. Pleading guilty to fraud, he was imprisoned in Singapore for six and a half years. In his autobiography, *Rogue Trader*, Leeson condemned the practices that allowed him to gamble with such large amounts of money unchecked (BBC Online 1999). This case confirms the desirability of having effective internal controls and risk minimisation practices in place.

In the following two chapters some of the steps that organisations can take to minimise the risk of fraud occurring are discussed. This chapter begins with an examination of fraud prevention policies in both the public and private sectors. It then looks at the use of Codes of Practice to prevent fraud. This is followed by a discussion in Chapter 6 of some of the procedures and technologies that can be used for fraud prevention. It should be noted that while, ideally, these measures would eliminate fraud entirely, such a goal is unlikely to be achieved, given the variety of ways in which fraud can be perpetrated. Instead, the purpose of fraud prevention policies should be seen as establishing procedures that enhance the possibility of detection so that people committing fraud are likely to be detected.[93]

91 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

92 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

93 Mr Rory Mulligan, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

Fraud prevention policies

It is often noted that responsibility for the prevention of white-collar crime, and particularly economic crime, lies in the first instance with upper-level management within organisations (Smith & Grabosky 1998; Ernst & Young 2003). If chief executive officers and managers at all levels have a commitment to the prevention of crime, and understand how that goal may be achieved, this will provide a foundation and model for their employees to follow.[94] While it is not possible to force people to have such a commitment to fraud prevention, it is possible to put in place policies and procedures that can encourage compliance with such an ethic, and help minimise the risk of fraud taking place.

Corporate governance

Such policies can be implemented at a number of different levels. At the broadest level, policies relating to good corporate governance can help address the issue of fraud. Standards Australia has recently released the first national consensus-based package of standards relating to corporate governance (Standards Australia 2003a, 2003b, 2003c, 2003d, 2003e). One of these standards, Standard AS8000-2003 *Good Governance Principles*, defines corporate governance as 'the system by which entities are directed and controlled'. It addresses 'the issues arising from the interrelationship between boards of directors, such as interaction with senior management, and relationships with the owners and others interested in the affairs of the entity, including regulators, auditors, creditors, debt financiers and analysts' (Standards Australia 2003a, p.8).

Of particular relevance to this Inquiry is the way in which corporate governance operates to hold organisations accountable for their activities. An organisation committed to good governance should have in place mechanisms that help to 'establish and maintain an ethical culture' (Standards Australia 2003a, p.6). This can be done in a number of ways. Some of the steps recommended by Standards Australia include: the development of a Governance Policy and a Code of Conduct; the development of clear procedures for the operation of the entity, including specification of the roles and responsibilities of Board members and directors; clear guidelines in relation to record keeping and internal reporting; and the creation of an Audit Committee (Standards Australia 2003a). Such steps should 'assist in the prevention of fraudulent, dishonest and/or unethical behaviour' (Standards Australia 2003a, p.7).

94 See, for example, Mr Dennis Challinger, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; and Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

The need for good corporate governance is seen by the Committee as being essential, especially in light of recent research revealing that most fraud is perpetrated by managers (KPMG 2002; Ernst & Young 2003; PricewaterhouseCoopers 2003). Such fraud may involve making purchases for personal use, misusing expense accounts or misappropriating funds (KPMG 1997). Some of Australia's largest corporate frauds have also been characterised by chief executive officers who exercise unfettered power and boards of directors who are unwilling to challenge them. This makes it difficult to establish effective codes of practice and create an ethical environment in some workplaces, because such initiatives directly challenge those in charge of the company who are themselves the main offenders (Smith 2002b). Good corporate governance policies and structures could help prevent this kind of situation arising, by ensuring that directors ask the right questions, that auditors are properly independent of the executive or senior management, and that external reviews are implemented where there are any doubts about the chief executive officer or other senior employees.[95]

Risk management

In addition to having broad governance policies in place, fraud prevention can also be addressed through the use of risk management policies. While corporate governance focuses on the entire structure of an organisation, risk management, as the name implies, merely focuses on the particular risks faced by an organisation. Standards Australia has also released a standard on risk management, which defines the area as follows:

> Risk management is the term applied to a logical and systematic method of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize opportunities (Standards Australia 1999, p.1).

Clearly, in many organisations one of the potential risks to be considered is the risk of fraud being perpetrated against the organisation, either by an internal or external party. A good risk management policy will examine the possibility of such a risk occurring, and take appropriate steps to prevent it.[96] This will generally be achieved by establishing mechanisms to guard against identifiable risks, and to enable problems to be detected once they have arisen. The steps to be taken will differ, depending on the nature of the organisation, and the particular risks faced: 'Risk management is about a structured approach to arrive

95 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

96 Mr Edward Hay, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

at a defensible internal control framework where you have the appropriate level of control to match the risks that you have'.[97]

It is likely that if risk management is done well, fraud control will also run well.[98] This is because a good risk management policy will address the risks of fraud faced by a particular organisation. It is possible, however, that such risks could be overlooked. It is for this reason that specific fraud control policies may also be necessary. Unlike risk management policies, which can be very broad-ranging depending on the particular organisation, a fraud control policy is very narrowly focused. Such a policy is intended to ensure that the organisation has specifically considered the possibility of fraud, and taken any steps necessary to address such a possibility.

Fraud control policies

In its package of corporate governance standards, Standards Australia has included a specific fraud-related standard, AS8001-2003 *Fraud and Corruption Control* (Standards Australia 2003b). This standard notes the increasing incidence of fraud in recent years, and states that 'controlling the risk of fraud…is a governance issue which must be given due attention by the controllers of all entities' (Standards Australia 2003b, p.4). It goes on to recommend a number of structural and operational steps that should be taken to minimise the risk of fraud, including comprehensive assessment of fraud risks, development of fraud control plans, the use of internal audits and pre-employment screening, and the implementation of whistleblower protection policies.

Corporate governance, risk management and fraud control are all clearly interrelated, as they all touch on the governance of an organisation. Ideally, every organisation would have clear, well-considered policies in each of these areas, constructed so as to complement each other. With a commitment to the implementation of such policies, it is likely that the incidence of fraud would be significantly reduced. Unfortunately, many organisations do not currently have such policies. The following sections examine the use of such policies in the public and private sectors and make recommendations about their implementation.

Public sector policies

With the onset of fiscal constraints during the late 1970s, Australian governments have become increasingly sensitive to the risks of economic crime. There has also been a recent recognition of the need to create an ethical environment in the public sector by educating public servants about the

97 Ibid.

98 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 3 July 2003.

desirability of complying with laws and codes of practice. In this sense, public servants may be seen as standing in a fiduciary relationship to the community and therefore their overriding duty is to act in the best interests of the community as a whole (see Mills 1999).

Government agencies are vulnerable to fraud from three main groups of 'outsiders': those who claim benefits to which they are not entitled; those who evade payments due to the government; and those who contract with the government to provide goods and services but who engage in deceptive practices (Smith 2002b).

Public sector agencies are also at risk of fraud from within. As noted above, a significant proportion of fraud is committed by management, as well as by employees. In particular, it has been noted that threats to information systems come disproportionately from within. As the Draft *National Strategy to Secure Cyberspace* in the United States, notes:

> Approximately 70 percent of all cyber attacks on enterprise systems are believed to be perpetrated by trusted 'insiders'. Insiders are trusted people with legitimate access rights to enterprise information systems and networks (United States, President's Critical Infrastructure Protection Board 2002, p.4).

Although the term 'cyber attacks' includes activity beyond the scope of the present discussion, the fact remains that it is important to have adequate structures and processes in place to deal with the threat posed by insiders, in both corporate and government settings.

Due to this concern about both external and internal fraud, many public sector agencies around the country now have detailed fraud control policies in place that provide guidelines on the establishment, implementation, and management of agencies in order to reduce fraud risks. This does, however, differ according to jurisdiction. A sample of the ways in which different jurisdictions have approached this issue is provided below.

Federal

Under section 45 of the *Financial Management and Accountability Act 1997* (Cth), Chief Executive Officers (CEOs) of federal Australian Public Service (APS) agencies are required to implement a fraud control plan for their agency. The CEOs have primary responsibility for fraud control within their agency, and for reporting fraud control activities to their Minister and in their annual report. The Australian government Attorney-General's Department has responsibility for the co-ordination of fraud control, and works closely with the Australian Federal Police.[99]

In 2000 the Australian National Audit Office (ANAO) (2000b) conducted a performance audit of fraud control arrangements in APS agencies. The audit

99 Ibid.

found that most APS agencies had a framework in place containing key elements for effectively preventing and dealing with fraud. The extent of these arrangements ranged from most agencies having undertaken fraud-awareness-raising activities, to a lesser proportion having specific fraud policies and fraud control plans in place and having undertaken risk assessments. It found, however, that about one-third of agencies had not undertaken a recent risk assessment to identify both the existing risks and those emerging as a result of the changing environment and methods of service delivery. The survey also found that 85 per cent of fraud committed occurred in less than 10 per cent of agencies.

Following this review, new federal *Fraud Control Guidelines* were released in May 2002 (Australian government Attorney-General's Department 2002). These guidelines outline the principles and standards of fraud control. Although the guidelines relate only to federal government departments, and do not encompass any enforcement function, they provide a consistent set of directions to assist departments in carrying out their responsibilities to combat internal fraud. These include agency responsibilities for fraud prevention, reporting of fraud information, investigation case handling and training of investigators.

The Federal *Fraud Control Guidelines* define fraud against the Australian government in Guideline 2 as 'dishonestly obtaining a benefit by deception or other means'. This explicitly includes theft; obtaining any benefit by deception; causing a loss, avoiding or creating a liability by deception; providing false or misleading information to the Australian government or failing to provide information where there is an obligation to do so; making, using or possessing forged or falsified documents; bribery, corruption or abuse of office; unlawful use of Australian government property or services; and certain bankruptcy offences. This list is non-exhaustive.

The benefits referred to can be either tangible or intangible, involving such diverse acts as hacking or interfering with an Australian government computer system, or using such a system to gain unauthorised access to another system; using a false identity to obtain income support payments; charging for incomplete or undelivered goods or services; hiding or disposing of assets by bankrupts to avoid paying creditors; and making false statements under the *Electoral Act 1918* (Cth).

The guidelines require agencies to undertake fraud risk assessments and produce fraud control plans at least every two years. Agencies are also encouraged to incorporate their fraud risk management into a general business risk management approach. In doing so, agencies are directed to take into account a number of standards in the area, including the Standards Australia *Risk Management* standard (Standards Australia 1999).

Australian Capital Territory

The ACT Government Service Fraud Prevention Unit has established a fraud control policy in accordance with the Public Sector Management Standards on Fraud Prevention. The policy sets out the responsibilities of managers and employees in relation to fraud control, describes the investigatory functions of the Fraud Prevention Unit, and details the procedures for reporting fraud and corruption. Section 9(t) of the *Public Sector Management Act 1994* (ACT) requires public employees to report suspected fraud, while the *Public Interest Disclosure Act 1994* (ACT) provides protection against reprisals for those who report fraud and corruption in good faith (ACT Government 1994).

New South Wales

In New South Wales, the Audit Office, in conjunction with the Premier's Department, developed a 10-point fraud risk management plan for NSW public sector agencies in 1994. Areas covered by this plan include:

- Integrated Macro Policy: Each agency should possess a fraud control strategy as a clearly identifiable instrument at the policy level, which sets out the agency's stance on fraud;
- Responsibility Structures: Organisational responsibility for the co-ordination, monitoring, ongoing review and promotion of the agency's fraud control strategy must be clearly defined and communicated throughout the agency to management and staff;
- Fraud Risk Assessment: A structured fraud risk assessment review addressing internal and external fraud risks should be conducted periodically;
- Employee Awareness: There should be a well-constructed program of ongoing initiatives, including education and training, to bring the issues of fraud prevention, detection and reporting to the attention of all employees;
- Customer and Community Awareness: The community should be made aware that fraud against agencies is not acceptable, and that perpetrators will be prosecuted;
- Fraud Reporting Systems: Procedures for dealing with the notification of fraudulent activity need to be developed and distributed to all potential complainants;
- Protected Disclosures: Measures should be taken to positively encourage fraud reporting and to protect those making disclosures against recriminations;
- External notification: Agencies need to develop clear policies and procedures for the reporting of fraud to relevant external authorities, such as the police;

- Investigation standards: Procedures need to be developed and provided to operational and internal investigating staff to avoid any uncertainty or confusion about how matters should be handled;
- Conduct and Disciplinary Standards: Employees need to be made aware that fraud will not be tolerated and that perpetrators will face disciplinary action (NSW Audit Office 1994).

In its three-volume publication, *Fraud Control: Developing an Effective Strategy*, the Audit Office provides guidance on how individual agencies should put this plan into practice. A Self-Audit Guide has also been developed to help managers analyse the effectiveness of their fraud control strategy (NSW Audit Office 1999).

The implementation of this plan has been monitored closely by the Audit Office of New South Wales. In 1998, for example, it examined responses from 158 significant agencies across New South Wales. Of these only 8 per cent were considered 'highly effective' in implementing the plan, though 49 per cent had implemented most parts of it. The report did, however, find general improvement in implementation of the plan among the Audit Office's 40 largest clients. In evidence provided to the Committee, the Performance Audit Director of the NSW Audit Office stated that the plan has now been generally accepted by most public sector agencies.[100] Other evidence provided to the Committee also advised that the New South Wales guidelines, when implemented, seem to be very effective at controlling fraud in the government sector.[101]

Victoria

Financial Management Package

At present, there is no specific fraud control policy for the Victorian Public Service (VPS). Instead, fraud control is one of the issues that falls within the scope of the general Financial Management Package (FMP). The FMP was developed and issued by the Department of Treasury and Finance in 1994. At its core are two pieces of legislation: the *Financial Management Act 1994* (Vic) and the *Audit Act 1994* (Vic). These Acts set up the general financial management framework for Victoria, as well as establishing the Office of the Auditor-General of Victoria. The stated purpose of the FMP is 'to improve financial administration and accountability and provide for annual reporting to the Parliament by all VPS entities' (Department of Treasury and Finance 2003a, p.4).

Under the framework established by the FMP:

100 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

101 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

> [P]rimary responsibility for the management and performance of individual entities rests with the relevant departmental Secretaries and statutory authority Boards. Consistent with this philosophy and approach, responsibility for the establishment of effective governance structures and arrangements, including those relating to risk/fraud management strategies, has been largely assigned to individual entities.[102]

While entities are primarily responsible for financial management under the FMP, the monitoring of financial matters is performed by the Office of the Auditor-General. This Office also assists in the development of financial management systems to ensure that expenditure is properly accountable and to encourage timely and accurate reporting of fraud.[103]

Other elements of the FMP include the *Financial Management Regulations 1994* (Vic) and a variety of Financial Reporting Directions. Of particular importance are the Standing Directions of the Minister for Finance (the 'Directions'), which have recently been revised, with the new version having taken effect from 1 July 2003. These Directions supplement the *Financial Management Act 1994* (Vic) and 'form the basis of sound financial management for the State' (Department of Treasury and Finance 2003a, p.8). They prescribe mandatory procedures that must be complied with by public sector agencies to implement and maintain appropriate financial management practices and achieve a consistent standard of accountability and financial reporting.

These Directions, and the FMP generally, take a broad approach to fraud prevention and control, focussing on the issues of corporate governance and risk management as a whole, rather than specifically looking at fraud. The underlying philosophy appears to be that if entities are properly governed, and risks appropriately managed, fraud will be minimised as a result. Consequently, the Directions do not expressly focus on fraud. Instead, they are divided into the following three general parts:

- Financial Management Governance and Oversight: The Directions in this part 'set standards for Public Sector Agencies, which should be incorporated as fundamental elements in an overall governance framework'. This includes Directions on implementing and maintaining a financial code of practice (Direction 2.1); establishing robust and transparent financial governance policies and procedures (Direction 2.2); establishing and maintaining an effective approach to the identification, assessment, monitoring and management of financial management risks (Direction 2.3); and establishing procedures in relation to internal and external audits (Directions 2.5 and 2.6).
- Financial Management Structure, Systems, Policies and Procedures: The Directions in this part 'set standards for all Public Sector Agencies to

102 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

103 Ibid.

achieve sound systems of internal control to support financial management'. This includes Directions on setting up a financial management structure with clearly defined roles and responsibilities, documented policies, and procedures for the accurate processing of authorised transactions (Direction 3.1); establishing an appropriate strategy for the use of information technology, including ensuring appropriate security controls are in place (Direction 3.2); and implementing and maintaining an effective internal control framework in relation to revenue collection, cash handling, bank accounts, expenditure and asset management (Direction 3.4).[104]

- Financial Management Reporting: The Directions in this part 'set standards for Public Sector Agencies to assist them in measuring and managing performance and to ensure financial management reporting is consistent with applicable statutory reporting obligations'. This includes Directions on implementing and maintaining timely, accurate, appropriate and effective reporting procedures (Direction 4.1); reporting requirements (Directions 4.2-4.3); and monitoring financial performance (Direction 4.4) (Department of Treasury and Finance 2003b).

While most of the Directions outlined above do not specifically mention fraud, it is clear that they implicitly require public sector managers to prepare and implement appropriate fraud management strategies to reduce the risk of fraud.[105] For example, while Direction 2.1 does not specify that the financial code of practice should include fraud-related provisions, matters that must be covered in the code include integrity, accountability and encouraging the reporting of unlawful or unethical behaviour. Similarly, Direction 2.2 requires the implementation of procedures that ensure a balance of authority so that no single individual has unfettered powers over the finances of the Agency, as well as arrangements to ensure that public funds are used 'with due propriety'. Agencies are also required under Direction 2.2 to appoint an Audit Committee to oversee and advise the Agency on matters of accountability and internal control. The Directions relating to risk management also clearly touch upon the issue of fraud, as discussed above.

The structures and processes required by Directions 3.1–3.4, such as those relating to implementing procedures for cash handling and expenditure, as well as the reporting and monitoring requirements in Directions 4.1–4.4, also

104 It should be noted that the Department of Treasury and Finance has also issued *Purchasing Card Rules for Use and Administration* (Victorian Government Purchasing Board 2002). These Rules establish policies for government departments and offices to follow in relation to the purchase of goods and services, including a procedure for investigating possible breaches. Guideline 3 to Direction 3.4.6 encourages Public Sector Agencies to apply the principles set out in these Rules.

105 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

clearly relate to fraud prevention and control. The relationship of these Directions to fraud prevention is noted in the introduction to Part 3: 'Underpinning the system of internal control is the financial management structure, systems, policies and procedures that contribute to reliable financial information and to the safeguarding of assets, including prevention and detection of fraud' (Department of Treasury and Finance 2003b, p.25).

Financial Management Compliance Framework

The system of corporate governance and risk management envisaged by the FMP was enhanced by the introduction of the Financial Management Compliance Framework (FMCF) on 1 July 2003. The aim of the FMCF is to assist public sector agencies 'meet their obligations and effectively monitor and review their overall performance in financial management' (Department of Treasury and Finance 2003, p.2). It does this through instituting a continuous assurance framework, which involves entity, portfolio and whole-of-government level monitoring and review of financial management.

The FMCF was developed in compliance with the Standards Australia Standard AS3806 *Compliance Programs*. AS3806 provides best practice guidelines in relation to systems and procedures, resourcing and responsibilities, reporting, maintenance and culture. Each of these elements is incorporated into the FMCF.

While there are a number of elements to the FMCF, the most significant change it has introduced into the Victorian financial management system is a mandatory certification process. Under this process, all public sector entities (including departments and public sector agencies) are required to send an annual certification letter (signed by the secretary or CEO) to the relevant Portfolio Minister, stating that they have observed the Directions, or noting any areas where they have not complied with an element of the Directions. A checklist is provided for this purpose (see Appendix G).

Once the certification letter and checklists have been forwarded to Portfolio Ministers, the portfolios must compile an annual portfolio summary, which raises any non-compliance matters that are seen to be of particular relevance. This summary is to be forwarded to the Department of Treasury and Finance, which can then work with departments to resolve systemic whole-of-government non-compliance issues. The Department of Treasury and Finance will produce a whole-of-government summary report of compliance with the Directions. The Minister for Finance is responsible to the Parliament for ensuring appropriate controls are in place across the VPS.

In addition to this certification scheme, it is important to note that Procedure (c) under Direction 4.3 requires the Auditor-General and the Minister for Finance to be notified of 'all cases of suspected or actual theft, arson, irregularity or fraud in connection with the receipt or disposal of money, stores or other property of any kind whatsoever under the control of a Public Sector Agency'. This requirement is discussed in more detail in Chapter 8.

The general risk management approach to fraud prevention that has been taken to date by the Victorian Government is supported by the Auditor-General:

> A broader policy direction reflects the increasing contemporary emphasis placed on having in place effective enterprise-wide strategies dealing with governance. In this scenario, maintaining sound fraud prevention and control practices is viewed as one, albeit important, element of the responsibilities of those charged with governing and managing public sector agencies.
>
> The Auditor-General supports an enterprise-wide approach to governance issues with fraud prevention recognised as one of a number of key requisites for sound governance practices in organisations. This approach does not dilute the importance of fraud management but rather is likely to lead to stronger management practices in the area. We consider that fraud management needs to be well integrated with risk management strategies and internal control systems to achieve optimum effectiveness. These elements complement each other in a management sense and their integration is facilitated when governance is viewed from an organisation-wide perspective.[106]

Representatives of the Office of the Auditor-General did note, however, that:

> [deciding] whether to formulate specific policy requirements in this area or to focus on ensuring adequate coverage within wider managerial responsibilities associated with corporate governance … [is a] dilemma faced by public sector policy-makers… [and that] a fraud-specific policy approach can be justified on the basis that it recognises the high standards of responsibility that attach to the management of public funds and that all losses through fraudulent activity should be avoided.[107]

In evidence given to the Committee, it was also noted that 'it would be a good idea to encourage and enhance the question of what you do with fraud within the set of guidelines'.[108] Mr Newlan of the Corporate Crime Liaison Group supported the introduction of specific fraud control guidelines, stating that such a policy 'would be a giant leap in the right direction'.[109]

Proposed reforms

While the Committee acknowledges that, if properly implemented, the current financial management framework may well adequately address the risks of

106 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

107 Ibid.

108 Mr Edward Hay, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

109 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

public sector fraud, it believes that these risks would be better addressed if all public sector entities (including departments, public sector agencies and local government) were required to develop specific fraud control policies. Such a requirement would ensure that all public sector entities specifically address the possibility of fraud, and the steps they will take to prevent and control it, which may not occur under the current scheme. It would also highlight the importance of preventing fraud, which is essential given the recent increase in fraudulent activity across Australia and internationally.

To address the Auditor-General's concerns about fraud prevention and control being integrated into the general risk management scheme established by the FMP, the Committee recommends that the requirement for entities to implement and maintain a fraud control policy be included in the Standing Directions of the Minister for Finance. The annual certification process established by the Financial Management Compliance Framework should also require entities to certify that they have complied with the relevant Direction.

The relevant Direction should require entities to specify in their fraud control policy procedures in relation to the prevention, detection, reporting and investigation of fraud. The policy should also specify steps to be taken in the event that fraud is identified (a fraud response plan). The Direction should also specify that, in developing their fraud control policies, entities should have particular regard to Standards Australia's Standard AS8001-2003 on *Fraud and Corruption Control*,[110] as well as to the New South Wales Audit Office's fraud control policy *Fraud Control: Developing an Effective Strategy*.

While the actual fraud control policies developed will vary between entities, depending on their particular circumstances and needs, the Committee agrees with the view expressed in the submission from the Auditor-General that:

> Effective fraud prevention strategies should, ideally, include:
>
> - periodically reviewing all functions and operations to assess an agency's exposure to the risk of fraud;
> - developing a comprehensive fraud management plan;
> - instilling a culture of ethical behaviour in the agency;
> - training management and staff in fraud awareness and prevention;
> - ensuring accounting and operational controls are effective; and
> - introducing mechanisms available for all staff to report fraud.[111]

110 This was suggested to the Committee by Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; and by Mr Mark Bezzina, Director, Communications, IT and eCommerce, Standards Australia, in conversation with the Committee, 25 June 2003.

111 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003, citing the Auditor-General's *Report on Public Sector Agencies,* February 2003, pp.25-6.

In addition, the relevant Direction should require policies to specifically address the risks of fraud involving electronic commerce. This is an area of particular importance, because 'failure to effectively compensate for the loss of certain traditional controls and processes in IT systems and applications may significantly increase the susceptibility of agencies to material fraud and error'.[112] It has been noted that obvious fraud control measures are sometimes overlooked in this area because of the speed with which electronic commerce procedures have been implemented, or simply because those in charge of fraud control do not fully understand the nature of the risks that arise (Smith & Urbas 2001).

The lack of specific electronic commerce-related fraud prevention measures was noted in KPMG's *Global eFraud Survey* (2001). It was found that 30 per cent of respondents reported not having adequate segregation of duties in place with respect to their electronic commerce systems, while 60 per cent did not perform security audits. Some 62 per cent did not carry out background checks on entities that assisted them in developing, maintaining and/or administering their electronic commerce systems, while 56 per cent did not carry out background checks on entities with which they did business electronically.

A model fraud control policy for the Victorian Public Service, including steps to be taken to minimise the risks of fraud arising out of the use of electronic commerce, should be developed by the Victorian Fraud Information and Reporting Centre (VFIRC). A need for 'best practice guidance' was noted in the submission from the Auditor-General, to help improve the effectiveness of an entity's governance strategies.[113] VFIRC could also offer entities assistance in drafting their fraud control policies.

Recommendations

6a. The Committee recommends that a requirement that all public sector entities (including local government) implement and maintain a fraud control policy be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standard AS8001-2003 *Fraud and Corruption Control* and the New South Wales Audit Office's *Fraud Control: Developing an Effective Strategy,* and should include elements relating to the prevention, detection, reporting and investigation of fraud, as well as containing a fraud response plan. It should also specifically address the risks of fraud arising out of the use of electronic commerce.

112 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

113 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

6b. The Committee recommends that all public sector entities be required to certify their compliance with the relevant fraud control direction in the annual certification process established by the Financial Management Compliance Framework.

Private sector policies

In the private sector, as in the public sector, the best line of defence against white-collar crime is self-help. In particular, the establishment of robust internal controls is seen to be the most effective way of minimising the risks of fraud in the private sector. This was noted in Ernst & Young's most recent fraud survey:

> We asked respondents to rank the factors most likely to prevent fraud or detect fraud. In line with previous years, internal controls remain generally accepted as the best way to prevent and detect fraud. In our experience of investigating fraud, there is more often than not an internal control which should have prevented or detected the fraud – but it was either over-ridden, or not properly understood by the staff responsible for the control (Ernst & Young 2003, p.6).

As noted above, one way in which effective internal controls can be established is through the development and implementation of a fraud control policy. In the past, the use of such policies in the private sector was relatively uncommon. For example, in the fraud victimisation survey conducted by Deakin University in 1994, only 27 per cent of those surveyed had fraud prevention policies in place (Deakin University 1994). More recently, however, perhaps in acknowledgment of the desirability of implementing effective internal controls, the use of such policies by the private sector has increased. This is supported by the 2002 Ernst & Young survey which found, for the first time in their surveys, that most organisations had formal fraud prevention policies, including codes of corporate governance, employee conduct and fraud response plans (Ernst & Young 2003). Indeed, a large industry exists that provides loss prevention and risk management services to the private sector, with many large accounting firms having departments or subsidiaries specialising in fraud prevention. Their products range from a total review of risk management practices to more narrowly focused consultancy on issues such as security of information technology systems.

Despite finding such an increase in the use of formal fraud prevention policies, Ernst & Young have formed the view that 'more could and should be done by those charged with corporate governance in fraud prevention and awareness' (Ernst & Young 2003, p.3). The Committee agrees with this statement. The Committee believes that fraud control policies should be implemented as widely as possible in the private sector. Such policies not only help establish effective procedures to minimise the risk of fraud but also show a high-level commitment to the prevention of fraud. This is vitally important, as ultimately

fraud prevention will require the development of a culture of intolerance to conduct of this nature throughout the community.

To assist in this goal, the Committee recommends that VFIRC should be charged with the responsibility of promoting the implementation of fraud control policies by businesses and corporations in the private sector, using Standard AS8001-2003 *Fraud and Corruption Control* as a model. VFIRC should also be provided with sufficient resources to aid organisations in drafting and implementing such policies.

The Committee also encourages the development of a certification scheme to certify private sector organisations that have complied with Standard AS8001-2003. Such a scheme would involve an independent assessment showing that the organisation has developed and implemented an appropriate fraud control policy. Organisations that pass this assessment would be able to display a particular 'seal of approval', which should engender confidence in those who deal with them that fraud will be minimised. A list of organisations that have had their policy certified could also be published on VFIRC's web site.

At present, SAI Global Assurance Services runs such a scheme in relation to a number of different Standards Australia standards, including those relating to quality management, environment management, occupational health and safety management, and information security management (http://www.sai-global.com/ASSURANCE/SECTIONS/certification/).[114] Organisations that have complied with these standards are entitled to display the 'five ticks' StandardsMarks. It is hoped that a similar scheme will be developed in relation to the newly released Standard AS8001-2003.

Recommendations

7a. The Committee recommends that VFIRC promote the implementation of fraud control policies by businesses and corporations in the private sector, using Standard AS8001-2003 *Fraud and Corruption Control* as a model. VFIRC should provide assistance to such organisations in drafting and implementing such policies if necessary.

7b. The Committee encourages the development of a fraud control certification service for the private sector, to certify compliance with Standard AS8001-2003 *Fraud and Corruption Control*. If such a service is established, its existence should be promoted by VFIRC and certification encouraged. A list of those organisations that have had their policy certified should be published on VFIRC's web site .

114 See also Mr Mark Bezzina, Director, Communications, IT and eCommerce, Standards Australia, in conversation with the Committee, 25 June 2003.

Implementation of prevention policies

When discussing the issue of fraud control policies in its most recent fraud survey, Ernst & Young stated that they were 'concerned that issuing a policy by itself is insufficient. People need to be educated and held accountable to these guidelines or their behaviours are unlikely to change' (Ernst & Young 2003, p.9). This sentiment was echoed in a document on fraud prevention strategies provided to the Committee by Mr Wayne Cameron, Auditor-General of Victoria, in which it was stated that:

> Fraud prevention involves more than merely compiling carefully designed fraud control policies. It also involves putting in place effective accounting and operational controls, and the maintenance of an ethical climate that encourages staff at all levels to actively participate in protecting public and private money and property (Victorian Auditor-General's Office 2000).[115]

The Committee agrees that it is necessary not only to develop fraud control policies but also to communicate and fully explain those policies in order to prevent misunderstandings as to their meaning and effect. Often policies are established but not adequately implemented or publicised. Of particular importance is the need to provide information to staff on aspects of computer security along with appropriate guidelines on reporting computer misuse and abuse.

Providing educational material concerning fraud prevention and reporting procedures on internal agency web sites is now widely practised in the public sector. In the survey of Commonwealth fraud control arrangements conducted by the ANAO, approximately 30 per cent of agencies used email, and 35 per cent used their Intranet or public databases to disseminate fraud control information to staff (Australian National Audit Office 2000b). The Committee encourages the dissemination of fraud control policies in this way. The Committee also encourages the broader education of management and staff through seminars and training sessions. This is discussed in more detail in Chapter 7.

It should be noted that a delicate balance needs to be struck between providing information to staff about strategies adopted to prevent fraud, and keeping such information private so as not to alert potential offenders to the security measures they will need to circumvent in order to perpetrate fraud. Unfortunately, experience has shown that those persons most likely to commit computer-related fraud are often upper-level staff who already have knowledge of an agency's security measures. This raises the need for agencies to monitor the activities of staff at all levels regularly, without infringing personal privacy.

115 This document was provided as an attachment to the submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

Codes of practice and guidelines

Codes of practice can also be used to set acceptable rules and procedures for preventing and responding to fraud. Not only are they able to provide a widely disseminated statement of existing laws and acceptable practices, which helps to create a culture of compliance within specific industries, but they also often include dispute resolution procedures and sanctions for non-compliance with the rules in question.

Victorian public sector codes

The Code of Conduct for the Victorian public sector is a useful starting point for the standards of behaviour expected of government employees. This Code is made under section 37(1)(a) of the *Public Sector Management and Employment Act 1998* (Vic). It was revised in August 2003, with the current version being published by the Office of Public Employment (2003).

Like other codes of conduct, the new Code 'outlines the standard of behaviour expected of public sector employees' (section 1). A number of these standards can help minimise the risks of fraud. For example, section 27 restricts the use of official resources, such as computers, email and the Internet, to 'official purposes only' (with limited exceptions), while section 24 specifically prohibits employees from sending fraudulent material by email.

Employees are also urged to:

> [R]eport any unethical behaviour or wrongdoing by any other employee to an appropriate senior officer. This may include behaviour that you believe violates any law, rule or regulation or represents corrupt conduct, substantial mismanagement of public resources, or is a danger to public health… (section 37).

And one of the guiding principles of the Code is that employees should:

> [M]aintain public trust by being honest, open and transparent in all dealings and by acting in the public interest. Avoid real or apparent conflicts of interest and report any improper conduct, corruption, fraud and maladministration at work (section 2).

Unfortunately, while the sentiments behind this Code are admirable, these principles alone are unlikely to be of great effect. For example, the prohibition in section 32 on taking 'improper advantage' of information gained in the course of employment is unlikely to deter a would-be offender, who would no doubt be fully aware that such actions are morally questionable, if not downright illegal. If the Code of Conduct is to be of effect, it is necessary that it be backed by appropriate sanctions.

At present there are no sanctions applicable for breaches of the Code of Conduct. It is uncertain what consequences if any would follow any breach of its provisions. The Committee believes that appropriate sanctions should be

included within the Code to reinforce the serious consequences of failing to comply with its provisions.

Recommendation

8. The Committee recommends that appropriate sanctions be introduced for failure to comply with the Code of Conduct for the Victorian Public Sector.

Private sector codes

Documents of a similar nature are also in use in specific private sector industries, some of them provided by government agencies. For example, the Australian Competition and Consumer Commission (ACCC) has developed Guidelines for Advertisers, while state and territory departments of consumer affairs also have guidelines on complying with local laws such as those relating to the protection of privacy.

Some industry groups also have their own codes of practice, such as the Australian Publishers' Bureau Advertising Code of Practice, which sets out its requirements for acceptable advertising in six short paragraphs. These codes and guidelines do not replace or detract from rights which consumers have under existing legislative regimes. However, since they often operate across traditional jurisdictional boundaries, they increase the possibility of uniform practices emerging despite legislative differences between jurisdictions.

Although many countries now have codes of practice to regulate online activities, Australia has been a leader in codifying desirable practices on the Internet. The following discussion is drawn from Grabosky, Smith and Dempsey (2001).

Advertising and marketing codes

Codes of practice established by the marketing and media industries in Australia have targeted particularly vulnerable groups of consumers such as children, as well as specific content and products such as obscene materials, therapeutic goods, tobacco and alcohol. The Media Council of Australia, for example, administers a variety of voluntary codes of practice relating to advertising of therapeutic goods, slimming products, alcohol and tobacco products (see Pearson 1996).

In December 1997 the Australian Ministerial Council on Consumer Affairs released the Direct Marketing Model Code of Conduct to regulate the conduct of those involved in the direct-selling industry. The Code is administered by the Australian Direct Marketing Association (ADMA). ADMA was established in 1966 as the peak industry body for companies and individuals engaged in direct marketing in Australia. The Code applies to telemarketing, mail-order and Internet sales. Membership of ADMA is open to corporations, organisations, charities and partnerships, while individuals are able to join as

associate members. In 1996 ADMA began providing a training program in competency-based direct marketing at certificate and diploma levels.

All ADMA members must undertake to abide by the voluntary Direct Marketing Code of Practice published by the Association, which seeks to ensure that direct marketing engaged in by members complies with the highest standards of integrity. The 'Standards of Fair Conduct' within the Code govern the making of an offer, identification of the advertiser, the use of incentives, the placing of orders, fulfilment of orders and the use of mailing and telephone lists. Arrangements are also made for the arbitration of disputes, and members agree to comply with all legal requirements governing their activities.

The Code also specifically refers to direct marketing carried on electronically, such as via the Internet. Clause D2 of the Code states:

> Clear, complete and current information about the identity of businesses engaged in electronic commerce and about the goods and/or services they offer should be provided to customers. Additional information should be provided to address particular aspects of digitized goods and services, such as technical requirements or transmission details.

Failure to comply with the code may result in members' conduct being investigated by a Code Authority established by the Association. Sanctions include orders requiring members to take remedial action or give an undertaking not to repeat the breach of the code, issuing a formal written admonition (and, for serious breaches, to publish it) or to recommend revocation of membership.

Internet industry and electronic commerce codes

The Internet Service Provider (ISP) industry has established a variety of industry-based organisations, a number of which have developed means of self-regulation. The Internet Industry Association (IIA), which evolved out of a working group of major telecommunications companies, is implementing several codes of practice (http://www.iia.net.au/codes.html). The oldest is the content code, now at version 7.2 (registered in May 2002), which was based on generally accepted international standards, such as Australian Standard AS-4269-1995, and a wide range of existing and related codes, including the Ministerial Department of Consumer Affairs' Guide to Fair Trading Codes of Conduct. The first version of a Content Code specific to Internet gambling services was implemented in late 2001. A Code on privacy has also been ratified by the IIA Board, and was submitted to the Federal Privacy Commissioner for registration in March 2003.

The two state-based Internet industry bodies that exist alongside the IIA – one in South Australia and the other in Western Australia – have their own Codes which their ISP members each undertake to observe. The Western Australian Internet Association's (WAIA) Code of Conduct, for instance, requires members to declare that they will not 'knowingly permit a user to engage in criminal

activity using access to my system' (Western Australian Internet Association 1997), and the South Australian Internet Association's (SAIA) Code of Ethics and Conduct states that all its members agree 'to act fairly, with integrity, conscientiously and honestly' (South Australian Internet Association 2002). These are very generalised obligations, and their observance is voluntary because they are part of membership, which itself is voluntary. The main measure to which a party in breach could be subject would be exclusion from their Association. Victoria does not have a comparable state-based Internet industry association.

An Internet Code of Conduct has also been created by the Consumer Affairs Division of the Commonwealth Department of Treasury, to deal specifically with business-to-consumer electronic commerce transactions. The code, *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business* (Department of Treasury, Consumer Affairs Division 2000), builds on the recommendations of the Council of the Organisation for Economic Cooperation and Development (OECD) concerning guidelines for consumer protection in the context of electronic commerce (OECD 1999). These OECD recommendations include a set of general guidelines to protect consumers participating in electronic commerce without erecting barriers to trade. They represent a recommendation to governments, businesses, consumers and their representatives as to the core characteristics of effective consumer protection for electronic commerce.

Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business sets out the responsibilities of businesses that trade online and provides guidance to businesses for enhancing consumer sovereignty by giving consumers information on what businesses should do when dealing with consumers over the Internet. It aims to increase consumer confidence in electronic commerce and provides guidance to industry and consumers on the elements of an effective self-regulatory framework. The model provides guidance on:

- fair business practices;
- advertising and marketing;
- disclosure of a business's identity and location;
- disclosure of a contract's terms and conditions;
- the implementation of mechanisms for concluding contracts;
- the establishment of fair and effective procedures for handling complaints and resolving disputes;
- adopting privacy principles;
- using and disclosing information about payment, security and authentication mechanisms; and

- the processes and policies necessary to administer a code based on the Best Practice Model.

A recent addition to the codes of practice intended to regulate this area is the draft *Cybercrime Code*, released for public consultation by the Internet Industry Association in July 2003. This Code was the result of negotiations with law enforcement agencies about ways in which the level of co-operation between police and ISPs throughout Australia could be enhanced (Dearne 2002). It is hoped that such a Code will help facilitate the investigation of cases relating to electronic commerce fraud and other cybercrimes in which the police require the assistance of ISPs. In evidence given to the Committee, Mr Alastair MacGibbon Director of the Australian High Tech Crime Centre supported the use of this Code, seeing it as a 'healthy start' to policing this growing area.[116]

The general question of how great a contribution to monitoring and law enforcement can reasonably be expected of ISPs is open to debate. The large volume of data moving through the servers of an average ISP on a daily basis makes both active monitoring and long-term storage virtually impossible. For example, an ISP may have 450 megabits per second passing through its server (four megabits of text is roughly the length of a novel).

It is possible, however, that certain types of fraud, such as that perpetrated by mass unsolicited email or 'spamming', could realistically be monitored. The Western Australian Internet Association has a 'Spam Code of Conduct' which states that a member 'shall not knowingly send … or permit their computer or network to be used to send' unsolicited bulk Internet communication (Western Australian Internet Association 2002). The Australian government has also recently passed the Spam Act 2003 (Cth) and the Spam (Consequential Amendments) Act 2003 (Cth), which seek to address the problem of mass unsolicited email. Contained within these Acts are specific provisions which allow the telecommunications industry to make codes of conduct relating to 'e-marketing activities', in an attempt to regulate what is seen to be a growing problem.

The Committee believes that codes of conduct can be particularly useful in regulating the use of the Internet and electronic commerce. To this end, the Committee recommends that existing nationwide codes, such as *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business* and the *Cybercrime Code* (when finalised) be widely promoted and implemented across Victoria.

The Committee also believes that it would be advantageous to have an Internet industry body in Victoria, similar to those existing in South Australia and Western Australia. Such a body could help regulate the Internet industry in Victoria and develop a Victorian Internet Industry Code of Conduct, which

116 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

could include provisions to deal with fraudulent content and unsolicited material transmitted electronically. It could also work with Victoria Police in implementing the *Cybercrime Code*, or in relation to other crimes committed electronically. It is important that any such Code contain appropriate sanctions for those who fail to comply with its terms.

Recommendations

9a. The Committee recommends that an Internet industry body be established in Victoria. Steps should be taken to facilitate the establishment of such a body, including the provision of seed funding if necessary. Any body that is established should be encouraged to develop a Victorian Internet Industry Code of Conduct which deals with fraudulent content and unsolicited material transmitted electronically.

9b. The Committee recommends the promotion and use across Victoria of the Department of Treasury's *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business*, as well as the Internet Industry Association's *Cybercrime Code* when finalised.

Online gambling codes

As mentioned in Chapter 4, the Interactive Gambling Industry Code has been developed by the Internet Industry Association in response to the provisions in the *Interactive Gambling Act 2001* (Cth). The Act requires ISPs to assist with the prevention of access by users to certain Internet content through the use of available technologies. It requires ISPs to provide new customers with filtering software that has been approved for use in Australia. As part of this obligation, ISPs must also provide them with adequate information to install and start using this software, or initiate the process as part of the registration of the customer. The Code also places some obligations on the Australian Broadcasting Authority to notify companies developing the filtering technologies of the information that will identify gambling content which is prohibited, to ensure that the software is continually updated to identify and filter this content.

Enforcement of codes

Non-compliance with codes of practice is an area of continuing concern, because most codes contain few, if any, sanctions for breaching their terms. Occasionally consequences of non-compliance are provided for, such as in the *Fair Trading Act 1987* (WA), section 44 of which provides that failure to comply with an industry code of practice may result in the Commissioner for Fair Trading requiring the individual to give an undertaking to discontinue the offending conduct, to comply with the code in the future, or to take action to rectify the consequences of the contravention. More serious consequences may include suspension or disqualification of the offending person from the

membership of the industry group in question, which could entail substantial financial consequences in terms of loss of reputation and contacts.

In most cases, however, there is little that can be done to enforce compliance with a code of practice. To address this problem, Part IVB (ss.51ACA to 51AE) was inserted in the *Trade Practices Act 1974* (Cth) in April 1998. These provisions permit industry codes of conduct, whether mandatory or voluntary, to be enforceable under the Act, with legal action able to be taken for breaches of the codes or specified parts of them. A similar scheme exists under Part 6 of the *Fair Trading Act 1999* (Vic). To date, the only code to be mandated under Part IVB is the Franchising Code of Conduct.

Given the substantial risks of electronic commerce and Internet-related fraud, the Committee recommends that codes in these areas should also be mandated under the *Trade Practices Act 1974* (Cth). This would help ensure that organisations that have agreed to comply with such codes of practice will take steps to do so – including complying with those provisions specifically aimed at reducing the occurrence of fraud. Non-compliant organisations risk incurring substantial penalties.

It should be noted, however, that even if these codes are mandated, they face the same limitation faced by all codes of practice: their operation is limited to those who have agreed to comply with their provisions. Although this may be adequate for large organisations, such as those involved in direct marketing, the controls are usually restricted to specific geographical regions. In the world of online marketing and advertising in which information travels so easily across borders, the possibility of consumers being misled by information from some overseas entity is greatly increased. There is also the possibility of conflicting guidelines being established in different countries to regulate essentially identical activities.

Ideally, in the global electronic commerce marketplace, groups representing similar interests will agree on international codes of practice. One could imagine, for example, that an international code of practice could be created which would apply to all entities engaging in electronic commerce throughout the world. Indeed, as noted above, the OECD has created a set of guidelines to enable self-regulatory regimes to be constructed along similar lines in different member countries (Bridgeman 1997). The problem that uniform international codes of practice face is ensuring that differences in local public sentiment can be accommodated in setting trans-jurisdictional standards. In regulating obscene and objectionable content, for example, this has proved to be a considerable hurdle (Butler 1996). In the field of misleading and deceptive practices, however, international consensus might be more easily achieved (Smith & Urbas 2001). The Committee supports attempts to achieve such consensus.

Recommendation

10. The Committee recommends that industry Codes of Conduct relating to electronic commerce, the Internet and online gambling be mandated under Part IVB of the *Trade Practices Act 1974* (Cth).

Conclusion

This chapter has focused on the different types of policies that public and private sector organisations should have in place if they want to reduce the risk of fraud. These policies are important not only because they can help establish internal systems and procedures that may be effective in minimising or preventing fraud, but also because they can help create a culture of intolerance. Such a culture is essential if fraud is to be addressed in the long term. The following chapter examines other procedures and technologies that can also assist in the creation of fraud-resistant organisations.

6. Prevention Procedures and Technologies

Introduction

Chapter 5 of this Report examined the use of fraud control policies and codes of practice to prevent fraud. While such policies can be important in establishing a general fraud minimisation framework, there are other measures that can also help to reduce the risk of fraud. In particular, a wide range of technological solutions has been devised for application in both the public and private sectors. These and other preventive measures form the focus of this chapter.

Information security management

Fraud often occurs as a result of individuals obtaining confidential information. For example, credit card fraud will generally arise where an individual obtains another person's credit card details without their authorisation. Identity-related fraud can involve the use of personal information, such as a person's birth date or mother's maiden name. Certain types of corporate fraud can also occur where an individual gains unauthorised access to sensitive information, often held on computerised databases. One of the simplest and most effective ways in which these types of fraud can be prevented is by protecting the information that is used to perpetrate the fraud. If there is no way of obtaining the information necessary to commit the crime, attempts at dishonesty will be thwarted at the outset.

The ways in which information can be protected vary depending on the nature of the information and who holds it. In the case of personal information, such as credit card information, bank account details or other information that could be used to perpetrate identity-related fraud, the protection of information involves taking simple measures such as those outlined recently by the Australian Institute of Criminology (2003):

- Not providing personal information and data to someone unless there is a reason to trust them. In particular, personal data should not be given

to people claiming to be from a bank or credit card company unless their identity can be verified;

- Taking care not to disclose personal information over the phone, or enter a PIN into an ATM or EFTPOS machine when someone is watching or listening;
- Not disposing of ATM debit and credit card receipts in public places, but instead taking them home to shred or destroy;
- Destroying expired documents such as drivers' licences, passports, credit cards and old financial records such as tax returns and bank statements;
- Using a locked mail box, and having mail held at a local post office or picked up daily by a trusted person if absent;
- Storing valuable official documents (such as passports and birth certificates) and financial and accounting records in a secure place; and
- Not carrying Tax File Numbers, PINs or passwords in a purse or wallet.

Where information is held by an organisation, however, it may be necessary to establish a more detailed information security management strategy. Such a strategy can set out procedures that are aimed at protecting all types of information, ranging from letters received by an organisation to the organisation's computerised accounting system. It is important to recognise that information security is about more than information technology. While it is obviously necessary to ensure that computer equipment is adequately secured from both internal and external attacks, it is sometimes just as important to ensure that paper documents lying on a person's desk are also secure.[117]

In order to provide best practice guidance on the development and implementation of such a strategy, Standards Australia has released a number of standards relating to information security management. These include AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management*; AS/NZS 7799.2:2003 *Information security management – Part 2: Specification for information security management systems*; and HB 231:2000 *Information security risk management guidelines*. These complementary standards set out a comprehensive system for the management of all types of information, and include provisions relating to organisational security, physical and environmental security, asset control, communications and operations management, and access control.

The aims of an information security management system are threefold (Standards Australia 1999). First, a secure information management system

117 Mr Mark Bezzina, Director, Communications, IT and eCommerce, Standards Australia, in conversation with the Committee, 25 June 2003; Mr Ray Bange, Acting Manager, Misconduct Prevention Unit, Queensland Crime and Misconduct Commission, in conversation with the Committee, 26 June 2003.

should ensure appropriate levels of confidentiality. Information should only be accessible to those authorised to have access. Secondly, such a system should ensure that the integrity of information is maintained. The accuracy and completeness of information should be safeguarded. Finally, it is necessary to ensure that authorised users have access to information and associated assets when required. Implementing such a system is seen to be vital, because:

> At the very least, failure to effectively manage information security can result in:
>
> - loss of business through loss of critical commercial information
> - exposure to legal actions for confidentiality breaches or supply of inaccurate information which leads to loss or damages
> - vulnerability to losses through computer fraud
> - losses through technical accident, ineptitude or malfunction
> - losses through fire and flood
> - losses through denial of service, hacking, computer viruses or other forms of industrial sabotage
> - losses as a result of links with faulty or insecure systems eg. partners or suppliers (SAI Global Assurance Services 2003, p.2).

There are a number of organisations that can assist in the development of appropriate information security management systems. For example, SAI Global can provide technical experts to examine an organisation's information security management processes, and provide feedback on where improvements can be made. A certification service is also provided for organisations that can demonstrate compliance with AS/NZS ISO/IEC 17799:2001 (see Chapter 5 on Certification Services). Certified organisations can display the relevant certification mark, which will inform customers, employees and other stakeholders that the organisation 'has invested in a system to meet the most widely recognised international benchmark standard of Information Security Management practices' (SAI Global Assurance Services 2003, p.3).

Many public and private sector organisations already have an information security management strategy in place. Large commercial organisations in particular are likely to have such a strategy, due to the need to protect the confidentiality of commercially sensitive information. There is, however, no requirement for organisations to implement an information security management strategy, and many organisations do not adequately protect their information. This can be seen in the results of the 1999 KPMG fraud survey, where poor physical security over computer equipment was found to be a common factor in allowing computer-related crime to occur (KPMG 1999).

Although there is no requirement for a general information security management strategy in the public or private sectors, the newly revised Standing Directions of the Minister for Finance (see Chapter 5) do contain some Directions that are relevant. In particular, Direction 3.2 contains a

number of requirements for public sector entities in relation to information technology, including ensuring that:

- where financial systems are connected to the Internet, controls such as firewalls, security logs and encryption are in place;
- back-ups are maintained for all financial management systems and data used, and are stored in an off-site, secure location;
- financial management systems have sufficient levels of security to ensure that only authorised people have access to transactions (Department of Treasury and Finance 2003b).

While these requirements may protect the security of some of an entity's information, information security management is about more than information technology, as noted above. The Committee believes it would be preferable for entities to have a complete information security management system in place that covers paper-based and electronic information. To this end, the Committee recommends that a requirement for entities to implement and maintain an information security management policy be included in the Standing Directions of the Minister for Finance. The annual certification process established by the Financial Management Compliance Framework (see Chapter 5) should also require entities to certify that they have complied with the relevant Direction.

The relevant Direction should require entities to specify in their information security management policy, procedures in relation to how information is processed, stored, transferred, archived and destroyed. The Direction should also specify that, in developing their information security management policies, entities should have particular regard to the Standards Australia standards in this area, including AS/NZS ISO/IEC 17799:2001, AS/NZS 7799.2:2003 and HB 231:2000.

The Committee believes that private sector organisations would benefit from developing and implementing such information security management policies. While the Committee does not recommend making such policies mandatory, the implementation by businesses and corporations in the private sector of information security management strategies that comply with the relevant Standards Australia standards should be promoted by the Victorian Fraud Information and Reporting Centre (VFIRC). VFIRC should also encourage businesses and corporations to have their information security management systems certified as being in compliance with the Standards Australia information security management standards. The Committee recommends that a list of those organisations that have had their systems certified should be published on VFIRC's web site.

If organisations are unwilling to implement such a strategy the Committee urges them to at least consider simple steps that can be taken to secure confidential information. For example, confidential information should not be

included unnecessarily in documents. In conversations held with representatives from American Express, the Committee was told that a review was currently being undertaken of all documentation sent to card members, to ensure that no useful account information was included. American Express is also looking at removing the middle four digits from receipts, so that account numbers cannot be ascertained.[118] The Committee encourages the continuing development of such measures.

Another relatively simple measure that could be taken is to avoid mailing confidential information where possible, to prevent it from being intercepted *en route*.[119] In addition, where it is necessary to make payments, the use of EFT rather than cheques should be encouraged, to reduce the possibility of cheques being stolen.[120] Finally, it is important to ensure that secure devices and appropriate levels of encryption are used for the transmission or storage of highly sensitive information.[121] This is particularly important in relation to financial information. Concerns were raised with the Committee that not all data passing to and from all EFTPOS and ATM machines is being protected with sufficient levels of encryption.[122] This creates the possibility that unencrypted or poorly encrypted information could be intercepted as it passes over telephone lines. To minimise this risk, the Committee recommends that all financial institutions operating in Australia make sure that all data moving to and from EFTPOS and ATM terminals is adequately encrypted.

118 Mr Bruce Cox, Regional Director, Global Security, American Express, in conversation with the Committee, 25 June 2003.

119 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, 24 June 2003.

120 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003. Mr Newlan noted in the evidence given that Telstra, as well as a number of other corporations, are now refusing to pay shareholder dividends unless they can provide a bank account number, to reduce the risk of cheques being stolen.

121 It was noted in the submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002, that the Pentagon in the United States has restricted employee use of personal wireless access devices for fear that they are too vulnerable to hacking.

122 Mr Bruce Cox, Regional Director, Global Security, American Express, and Mr Jilluck Wong, Regional Director, Fraud Prevention, American Express, in conversation with the Committee, 25 June 2003.

Recommendations

11a. The Committee recommends that all public sector entities (including local government) be required to implement and maintain an information security management policy and that this requirement be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standards AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management;* AS/NZS 7799.2:2003 *Information security management – Part 2: Specification for information security management systems*; and HB 231:2000 *Information security risk management guidelines*.

11b. The Committee recommends that all public sector entities (including local government) be required to certify their compliance with the relevant Information Security Management Direction in the annual certification process established by the Financial Management Compliance Framework.

12a. The Committee recommends that VFIRC promote the implementation of information security management strategies by businesses and corporations in the private sector, using the Standards Australia Information Security Management Standards as a model.

12b. The Committee recommends that VFIRC should also encourage businesses and corporations in the private sector to have their information security management systems certified as being in compliance with the Standards Australia Information Security Management Standards. A list of those organisations that have had their systems certified should be published on VFIRC's web site.

13. The Committee recommends that all financial institutions operating in Australia encrypt all data moving to and from EFTPOS and ATM terminals.

Authentication

Although ideally an effective information security management strategy will prevent people from obtaining information that can be used for fraudulent purposes, it needs to be acknowledged that such measures will not always be effective. Particularly in the area of identity-related fraud, there is an ongoing risk that people will be able to obtain sufficient information to take over another person's identity, or to create a new identity. Fraud involving the use of such fictitious identities, as noted in the previous chapters, is a growing problem around the world, and is causing significant loss to those involved.

Identity-related fraud takes place when an offender defeats the user authentication strategies of a system, whatever they may be, and successfully identifies himself or herself as someone else, whether in the guise of a real other person or under cover of a totally fabricated identity. Where user authentication procedures are circumvented, the offender can avoid responsibility for his or her actions. One way in which to address this problem is to improve the

methods by which people are identified, or authenticate their identity, so that people who attempt to use false identities are likely to be detected. This is seen to be essential to fraud prevention: 'Fundamental to this whole problem of commerce and crime, particularly e-commerce, is knowing who you are dealing with.'[123]

Human identification has been defined as 'the association of data with a particular human being' (Clarke 1994). It has been observed that 'the science of human identification provides three basic means of identification; namely, knowledge-based, biometrics and tokens' (Willox & Regan 2002, p.1). These might alternatively be described as what the person knows, who the person is, and what the person has (Potter 2002).[124] To a greater or lesser extent, various organisations currently use each of these systems. For example, most organisations use knowledge-based authentication on a daily basis, when users are required to log onto their computer network by entering a password or PIN that only they should know. Similarly, many organisations use token-based authentication when they limit access to their premises to those who hold the appropriate security passes. Biometric systems, such as those which identify users by recognising their fingerprint or iris pattern, are also becoming increasingly common. The simple use of a handwritten signature is also a biometric user authentication system.

Each of these systems, however, has particular weaknesses. For example, knowledge-based systems can be overcome if another person learns the relevant information, while token-based systems are vulnerable to theft or forgery. Even biometric systems, which are seen as more secure, can be deceived in a number of ways. For example, a fingerprint recognition system could be circumvented through the use of a fabricated finger. The following sections will examine some of the weaknesses of each of these systems, and make recommendations about ways in which authentication systems can be improved.

Knowledge-based systems

Knowledge-based systems are one of the most common ways in which an individual's identity is currently authenticated. It has been estimated that '98 per cent of companies still use passwords as the primary method of authentication internally. A roughly similar percentage of e-business sites use passwords as the primary method of client authentication' (National Office for the Information Economy 2002, p.4). People are often required to provide passwords when logging onto their work computers, to key in PINs when

123 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, 24 June 2003.

124 A fourth authentication system not covered by the three categories noted above is based on location – where the user is. It makes use of space geodetic methods to authenticate the physical locations of users, network nodes and documents. Users can thus be located at the time they attempt to gain access to a system, which provides a safeguard against individuals pretending to be legitimate users who are located in a different physical location (Denning 1998). Such methods of authentication are not in common usage at this time, however, and will not be discussed further in this Report.

seeking access to their bank accounts, or provide their birth date or mother's maiden name when identifying themselves over the telephone.

The reason why knowledge-based systems are so commonly used is because they are very cheap to implement. There is no need to issue any type of token, such as a licence or security pass. Apart from IT support, password-based authentication usually requires no third party products or services. They are also seen to offer a modicum of protection against identity fraud. It is assumed that only a limited pool of people will know the relevant information, and so some assurance is given when individuals can correctly provide information which identifies them as who they say they are.

Unfortunately, knowledge-based authentication systems are usually not very secure. This is because of the ease with which it may be possible to ascertain the relevant pieces of information. People often share passwords or PINs with their friends or co-workers. Alternatively, they might write them down, or use an obvious word such as their pet's name, despite warnings to the contrary. An individual may watch the person entering their PIN into a machine (with or without the aid of technological devices) – so-called 'shoulder-surfing' – or overhear them say their password on the phone. Practices such as 'dumpster-diving' (as it is known in the United States), which involve searching through an individual's rubbish for any such information, may also reveal the necessary material.[125]There are also computerised systems that 'crack' passwords by enabling computers to systematically search entire dictionaries in search of a password. Even if passwords are encrypted so as to prevent them from direct exposure, encryption keys have been broken through the application of massive computing resources, sometimes involving multiple networked computers to increase processing power and capacity (Denning 1998). It is generally not difficult for a determined identity thief to obtain the relevant information.

A number of technological systems have been devised in an attempt to enhance the security of knowledge-based systems. Systems have been devised which change passwords regularly or which deny access after a specified number of consecutive unsuccessful tries. Some work-stations have automatic shutdown facilities when they have not been used for a specified number of minutes. Single use passwords, where the password changes with every successive log-in, according to an agreed protocol known to the user and system operator, are also available.[126]

Challenge-response protocols may also be used as a means of carrying out user authentication. These protocols involve users providing evidence of their identity, which is subsequently confirmed by the system asking for additional information. This can either be done manually or automatically. Under a

125 Mr Clive Summerfield, Manager for Government Services, VeCommerce, in conversation with the Committee, 24 June 2003.

126 Mr Summerfield explained that such a system could be combined with voice recognition technology to enhance the security of such a system (Mr Clive Summerfield, Manager for Government Services, VeCommerce, in conversation with the Committee, 24 June 2003).

manual system, once users have provided their name and password they might be randomly asked a question based on information in their file, or on a number of 'secret phases' previously provided to the organisation. An automatic system is based on a public key infrastructure in which a user will be provided with a private key on a hardware device. The server then generates a random number that is sent to the user to key into the device. The device uses the private key to process the random number and to produce a result to return to the server. The server then validates the number returned (National Office for the Information Economy 2002).

Alternatively, call-back devices may be used. After the user dials into a computer through a modem and gives his or her name or 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 proceed. However, even this relatively sophisticated system can be overcome by the use of call-forwarding arrangements (Denning 1998).

Despite the existence of so many different options, many organisations rely upon the relatively insecure use of simple unencrypted passwords. This was identified as a problem to the Committee, with a need for better management of passwords and other access controls for computerised systems and applications being identified.[127] One way in which this could be achieved is through the implementation of a password management policy. Such a policy could cover:

- length (specifying a minimum number of characters for the password);
- use of dictionary words, extended characters, numbers, mixed case (a secure policy would ban dictionary words and force a mixture of all other characters);
- expiry period (passwords must be changed within a set period, often 90 days);
- history (records kept of password access attempts);
- grace logins (can users ever log in without a password, and if so, how often?);
- number of failed attempts (before the password is cancelled permanently);
- issue and re-issue procedures; and
- suspension (National Office for the Information Economy 2002, p.5).

The Committee encourages the use of such a strategy by both public and private sector organisations. Password management, and authentication as a whole, should be considered by the public sector when developing fraud control and information security management policies. VFIRC should also promote the use

127 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

of such strategies in both the public and private sector, and should be responsible for developing a best practice guide (see Recommendation 22b).

Organisations should also be encouraged to carry out a risk assessment procedure, to help determine the exact type of authentication system that should be implemented. This would involve an examination of the authentication needs of the organisation, including the level of security required, the size of the organisation, and the frequency with which such systems are used.

It should be noted, however, that although such strategies can help reduce the risk of knowledge-based systems being compromised, it is the users who are best placed to protect themselves from such risks by taking basic security precautions to ensure that access codes and other personal information are not stolen. Simple precautions such as not choosing obvious numbers, not sharing numbers and changing numbers regularly are recommended. Unfortunately, although many of these steps seem obvious, studies reveal that between 20 and 70 per cent of people are negligent in using access code information (Sullivan 1987). To help address this problem, the Committee recommends that VFIRC conduct a mail-out to all Victorian households of an information brochure on prevention methods that could be used to help minimise the risk of fraud victimisation in consumer transactions, business transactions, and electronic transactions, highlighting the importance of the responsible maintenance of passwords and PINs (see Recommendation 22b(i)).

Token-based systems

The main problems facing a token-based identification system are theft and forgery. It is possible for an individual either to steal another person's documents and use them as their own (with or without modifications), or to create fraudulent documents which can then be used as evidence of identity. While increasing use of technology has provided some protection against counterfeiting, through the incorporation of various document security features, the possibility of theft remains a problem. Similarly, with advances in computer technology, it is sometimes possible to bypass even the most secure systems and counterfeit documents containing the appropriate security features (Smith 1999).

Evidence of identity documents

In Australia, the *Financial Transaction Reports Regulations 1990* (Cth) established the so-called 100-Point system in which proof of identity documents used to open an account with a financial institution are assigned a value depending on their level of security. This system is currently undergoing assessment and review which, at the time of tabling this Report, remains incomplete. However, the key features of the existing system can be described, as it remains the basis of establishing the identity of individuals for a wide range of financial and other purposes when dealing with government departments. The notion of a points-

based system is also used in purely commercial settings, even in connection with the hiring of a videotape, although lower level documents would be appropriate for such transactions.

Under the current regulations, 'primary documents' are worth 70 points and include certificates of citizenship, current passports and birth certificates, while 'secondary documents' include drivers' licences, public employee or student ID cards (40 points each), credit cards, Medicare cards, and council rates notices (25 points each). There is a range of other documents that can be relied on to verify one's name and address, each carrying point values.

At present, 100 points of documentation are required in order to open an account with a financial institution, with higher numbers of points being required in order to establish one's identity for the most secure forms of electronic communications with the government under the Australian government's *Gatekeeper* Strategy.

The Strategy, as amended, specifies that the evidence of identity documentation for all certificate grades and types should comprise one primary document worth 70 points (birth certificate or passport or citizenship certificate) and one – or a combination of – secondary document(s) to achieve a minimum overall total of 100 or 150 points (as required). In addition, certain other conditions are specified. If a current photograph is not provided with a primary document then it must be provided as part of a secondary document, and where a name shown in a primary document differs from the name shown in a secondary document, proof of the reason for that name change must be provided. This proof does not count towards the 100-point check.

For all organisational certificates, organisational document(s) must be presented which identify the organisation, confirm that the Authoriser is a member of the organisation, and indicate that the Authoriser has approved an Authorised Officer for the organisation. The organisational documents recognised by *Gatekeeper* are an original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the business entity's name and the ABN. If, however, either the owner, chief executive or other officer or employee is named as the Public Officer on the document issued by the Registrar of the ABR, and if this person has clear capacity to commit the business entity, then this document only will suffice. A secondary check involving online verification with the ABR to link the organisation's ABN to its business name is recommended. Alternatively, if the notice issued by the Registrar of the ABR cannot be provided then a legal or regulatory document binding either the Authorised Officer or the Authoriser with a clear capacity to commit the business entity, to the business entity. In this case online verification with the ABR to link the organisation's ABN to its business name *must* be achieved.[128]

128 See http://www.noie.gov.au/projects/confidence/Securing/EOI%20Requirements.htm for the complete evidence of identity requirements under *Gatekeeper*.

Under the current Financial Transaction Reports Regulations 1990, special provisions 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 two years' imprisonment (*Financial Transaction Reports Act 1988* (Cth) s.24). It is also an offence knowingly or recklessly to make a false or misleading statement in advising a financial institution of a change of name, which carries a maximum penalty of four years' imprisonment (s.21A). Penalties also apply to cash dealers who fail to comply with reporting requirements under the Act (ss.28-34).

The 100-point system does not, however, provide a complete solution to the problem of identity-related fraud, as it is possible to submit evidence of identity documents that have been forged or altered. Although the Committee heard evidence that a system of validating identity through the use of documents of varying points depending upon levels of security was not, of itself, flawed,[129] it was also informed about how easy it was for counterfeit or altered documents to be used when seeking to satisfy the 100-point system.[130] The solution to the problem was seen not in increasing the number of points required for specific activities, but rather in improving the security of the documents used as evidence of identity and also enabling the verification of documents with the issuing source.[131]A report by the House of Representatives Standing Committee on Economics, Finance and Public Administration (2000) recommended, among other things, that the Australian Taxation Office improve its internal processes for establishing identity and preventing identity fraud and that the Australian government formalise a process for working with other levels of government and industry to develop options for reducing and preventing identity fraud. These reforms are currently being undertaken.[132]

In addition, as part of the Australian Government's initiative to combat identity-related fraud, many federal agencies are working towards the development of a common set of documents of higher integrity that will be used in the 100-point system. At the same time a common and transferable identity authentication framework is being investigated at federal level. On 7

129 Ms Liz Atkins, Deputy Director, Australian Transaction Reports and Analysis Centre (AUSTRAC), Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

130 For example, Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

131 Ms Liz Atkins, Deputy Director, Australian Transaction Reports and Analysis Centre (AUSTRAC), Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

132 Mr Chris Barlow, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, Canberra, 24 June 2003.

July 2003, for example, the Federal Minister for Justice and Customs announced the idea of a national 'Electronic Gateway' to enable data to be compared between all agencies that issue documents used for establishing identity such as birth certificates, drivers' licences, passports etc. If this is implemented, some of the problems of identity fraud would be resolved, but by no means all. Trials of the use of biometric identifiers for use in conjunction with proof of identity procedures have also taken place (Cuganesan & Lacey 2003).

At the same time, efforts are being made to cleanse existing databases of erroneous information held about registrants.[133] This will not only remove fictitious entries that could be used for fraudulent purposes, but will also remove entries which have incorrect information entered by mistake, or information that is no longer current (such as the retention of information concerning deceased people – which is occasionally used for fraudulent purposes).

In the wake of the September 11 attack on the United States, national security has been emphasised as a major priority in many countries. Among the measures being considered in some countries is the use of compulsory identity cards. Technology now provides the ability to establish such national identification systems through the use of Internet-based networks, and the needs of electronic commerce and electronic service delivery by government agencies also suggest that a national identity database might be beneficial. Proposals for the introduction of national identification cards are being discussed in the United Kingdom, South Africa and a number of South-East Asian countries in order to contain the risks of identity fraud and to enhance national security. For example, it was reported in early 2002 that Hong Kong would begin issuing multi-use ID 'smart cards' to citizens from July 2003, replacing all 6.8 million existing ID cards by March 2007. The smart cards will contain basic biometric information such as thumb-prints and a photograph and will be capable of multiple functions, including use as drivers' licences and as library cards (Benitez 2002).

Such proposals face vocal opposition by privacy advocates who raise the grave consequences of essential information being misused, such as occurred during the Nazi regime in the Second World War. One writer refers to 'the singular ease with which population registration systems have been mobilized for genocidal purposes' (Seltzer 1998, p.544). Responding to a recent British proposal for an 'Entitlement Card' released by the Home Office in July 2002 (Home Office 2002), a consultation paper by Privacy International observed that 'no common law country in the world has ever accepted the idea of a peace-time ID card' (Privacy International 2002). However, a pilot program for a biometric ID card on a much smaller scale has already been implemented in Britain in relation to asylum seekers:

133 Mr Graham Austin, Manager, Fraud Minimisation, NSW Registry of Births Deaths and Marriages, in conversation with the Committee, Sydney, 25 June 2003.

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

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

Rather than creating a single national identification system the Committee believes that it would be preferable to improve the security of the main documents used to establish identity, such as birth certificates, passports, and drivers' licences, and to exclude from any points-based system documents that fail to have adequate security measures in place. Already, for example, New South Wales has a plastic card birth certificate available that contains a photograph as well as other security measures. Verification checks between issuing agencies should also be enhanced to enable anomalies to be detected.

Recommendation

14. The Committee recommends that individual identification cards should not be introduced at a national or state level in Australia.

Document validation

There are various solutions to the problem of fraud committed through the use of counterfeit identification documents. First, and perhaps most important, is the need to validate identification documents 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 in each jurisdiction – there being no national registry presently (see the discussion on 'Identity-related fraud' in Chapter 2). An electricity account tendered as an identification document should be validated by checking with the electricity company concerned.

Exercising a degree of caution about customers seeking to obtain goods on credit is clearly the best defence against fraudulent activities involving abuse of credit facilities (Levi 1981). Because fraudsters often provide false business addresses and telephone numbers for trade referees, it is essential that referees be contacted and that independent information be obtained to verify the legitimacy of the contracting party (Churchill 1997). Conducting thorough checks on the financial standing of business clients to whom credit is extended is also obviously prudent.

Another key area for inter-agency co-operation concerns the verification of proof of identity documents. At present, documents used to establish identity are issued by a number of state and Commonwealth agencies as well as companies in the private sector. Cross-validation enables inconsistencies to be ascertained and identity-related fraud minimised. In addition, as one submission received by the Committee noted, improved identification checks are needed when corporations and businesses are registered and when accounts with public sector agencies, such as the Australian Taxation Office, are established.[134] All this requires considerable co-operation between the various layers of government. The ever-expanding incidence of identity-related fraud has, however, motivated a degree of federal and state and territory co-operation rarely seen. As Detective Inspector Colin Dyson of the New South Wales Police Service Fraud Squad stated:

> It should be recognised that the most effective strategy to prevent identity fraud involves a systemic strengthening in the control of processes, on a national basis, of all parties involved in identification use, for example, identification issuers, accepters, and users. These controls would be supported by effective policing strategies which must also be co-ordinated nationally (Dyson 203, p.15).

Perhaps the two most important documents used in identification procedures are birth certificates and drivers' licences. Both are valued at 70 points in the 100-point system and have various counterfeiting prevention devices in place. In a survey conducted by the Australian Bankers Association in 1999, it was found that drivers' licences were presented most often when opening accounts with financial institutions (in 31% of cases) while birth certificates were produced in 8 per cent of cases. Other commonly used documents were passports (22%), credit/debit cards (22%), and Medicare cards (15%) (Cuganesan & Lacey 2003). In a trial conducted by Westpac and the New South Wales Registry of Births, Deaths and Marriages of a Certificate Validation Service, it was found that 'in the particular instances where a birth certificate was tabled to the bank as part of the identification documentation, some 13 per cent were found to be false' (House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, p.67).

Following this trial, the New South Wales Registry of Births, Deaths and Marriages developed a birth certificate validation service. This online computer system enables birth, death, marriage and change of name certificates issued by the Registry to be validated by organisations that rely on the certificates as evidence of identity. Once particulars have been entered into the system, a Yes/No result is given which then allows further checks to be undertaken as required. Because no identifying information is actually provided by the Registry, individual privacy is not infringed. The Committee heard that the New South Wales Registry of Births, Deaths and Marriages has examined over

134 Submission (name withheld) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002. See also Cuganesan and Lacey 2003.

500,000 inquiries concerning its birth certificates, and has identified over 400 counterfeit certificates being tendered as evidence of identity.[135]

In February 2002, this validation service was extended to include certificates issued by the Victorian Registry of Births, Deaths and Marriages. Approximately 60 invalid Victorian birth certificates have been identified to date.[136]

Similar validation services are needed for other key proof of identity documents, particularly drivers' licences. Although these documents are not created for use as evidence of identity, they do take on this function. Agencies therefore need to take steps to ensure that counterfeit and altered documents are quickly identified and eradicated.[137] Arguably the ability to validate documents with the issuing source needs to be made available to certain private sector organisations as well as other government departments. In giving evidence to the Committee the General Manager of Pro Active Strategies stated that verification of documents is essential in carrying out pre-employment screening procedures.[138]

Recommendations

15a. The Committee recommends that a national approach be taken to the verification of documents used to establish identity, and encourages the Victorian government to co-operate fully with Australian government initiatives designed to enable the online verification of evidence of identity information and to improve the '100-point system' established under the *Financial Transaction Reports Regulations 1990* (Cth).

15b. The Committee recommends that public sector agencies and private sector organisations which issue documents that can be used as evidence of identity (such as birth certificates and driver's licenses) take steps to cleanse their databases of information to ensure that information is accurate and current, and that they co-operate with the development of online verification systems.

Document security

Because many crimes of dishonesty involve counterfeit or altered documents, the Committee believes that steps should be taken to enhance document security, in particular with respect to documents used for identification purposes. The Committee heard evidence of the level of sophistication and organisation being adopted by criminal groups to counterfeit and alter

135 Mr Graham Austin, Manager, Fraud Minimisation, NSW Registry of Births Deaths and Marriages, in conversation with the Committee, Sydney, 25 June 2003.

136 Letter from Mr Yehudi Blacher, Secretary, Department for Victorian Communities, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 9 December 2003.

137 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

138 Mr Shane Ringin, General Manger, Pro Active Strategies Pty Ltd, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

documents, due in part to developments in computing technologies that make scanning, alteration and printing of counterfeit documents relatively easy. The Acting Detective Superintendent of the Commercial Crime Agency of Western Australia Police noted the problem of organised crime groups continually targeting document-issuing agencies and using professional printing businesses to print high-quality fraudulent documentation in bulk.[139] Fraud has also been facilitated by organisations unnecessarily providing information such as actual signatures of their key personnel, corporate logos and letterheads on public web sites, all of which can be down-loaded for exact reproduction.

However, a large industry has now developed for the manufacture of document security technologies, and another industry is involved in training people in the detection of counterfeit and altered documents. Among these new technologies are security printing, in which colour-coded particles are embedded into the medium; 'tracer fibre', which can be woven into textile labels; and hidden holographic images, which can be read with a hand-held laser viewer or machine reader, thus permitting verification of a product's origin and authenticity. Other security features include embedded water marks, micro printing, copy protection and thermochromatic ink patches that change to white when a thumb is placed on them.[140] The use of these technologies makes counterfeiting extremely difficult although by no means impossible, particularly if confederates within issuing organisations assist in supplying precursor materials used for the manufacture of secure documents.

The Committee heard that the problem of counterfeiting of birth certificates is being addressed with the introduction of standard procedures to secure paper stock used for birth certificates and the use of individually numbered and bar-coded paper.[141] When such standardisation becomes nationally implemented it will be possible to ensure that all birth certificates are on standardised paper and have recognisable security features. This will facilitate the identification of counterfeits, but will also increase the levels of security required for organisations involved in the production of secure paper stock.

Similarly, as plastic card security is enhanced, greater physical security will be needed at businesses involved in the manufacture and issue of new cards. There have already been a number of burglaries from agencies that issue drivers' licences, resulting in stocks of licences being stolen that have subsequently been used in crimes of dishonesty.[142]

---

139 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

140 Letter from Mr Yehudi Blacher, Secretary, Department for Victorian Communities, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 9 December 2003.

141 Mr Graham Austin, Manager, Fraud Minimisation, NSW Registry of Births Deaths and Marriages, in conversation with the Committee, Sydney, 25 June 2003; Letter from Mr Yehudi Blacher, Secretary, Department for Victorian Communities, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 9 December 2003.

142 Mr Bruce Cox, Regional Director, Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003.

One particular risk arises when documents that can be used as evidence of identity are sent in the mail. It is possible that such documents could be intercepted en route, either at the Post Office or at the point of delivery. The Committee was advised that the Victorian Registry of Births, Deaths and Marriages mails approximately 220,000 birth certificates annually.[143] Given the large number of certificates that are mailed, the Registry has taken some steps to prevent theft, such as removing features from envelopes that would identify the mail as having been sent by the Registry. The Registry has also been discussing alternate delivery options with Australia Post.[144] The Committee encourages the development of alternative procedures to minimise loss and misappropriation of documents in transit, including minimising the extent to which documents are sent to clients by ordinary mail.

The Committee also heard of the need for enhanced levels of training for staff involved in validating documents, in order for them to be able to recognise legitimate evidence of identity documents as well as counterfeit or altered documents.[145] This, of course, presents a challenge for counter staff whose responsibility it is to check documents that are presented, as often there is insufficient time in which to inspect documents with precision. Rejecting legitimate documents wrongly can lead to complaints by customers and potential loss of business to organisations. Therefore members of the public need to be educated about the desirability of allowing time for documents to be thoroughly checked and for verification procedures to be undertaken. It is hoped that when customers understand that these checks are being conducted to prevent their own victimisation they will become more tolerant of delays and inconvenience.

In addition to document security and training, the Committee heard of some innovative practices that businesses have adopted to prevent document-based fraud. These involve changes to business practices, rather than simple document security. For example, in order to prevent refund fraud, some retail businesses refrain from giving cash refunds but instead only allow an exchange of goods, with colour-coded refund credit notes being provided, some with individual barcodes. Although such strategies could be circumvented by the on-selling of credit notes or refund vouchers, this would limit some of the more obvious risks of refund fraud.[146]

143 Letter from Mr Yehudi Blacher, Secretary, Department for Victorian Communities, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 9 December 2003.

144 Ibid.

145 Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

146 Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

Recommendations

16a. The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to ensure that effective security measures are used in those documents to minimise the risk of documents being altered or counterfeited.

16b. The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to comply with high level standards with respect to the security of materials used for the creation of such documents (including blank paper, inks, and plastic cards and their components), and that issuing branch offices be required to adopt uniform security standards .

16c. The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity take steps to minimise the extent to which documents are sent to clients by ordinary mail, and that alternative procedures be developed to minimise loss and misappropriation of documents in transit.

Biometrics

Biometric user authentication is one of the three basic systems of identification noted above. Biometric systems seek to identify a person based on who they are, rather than what they have or what they know. This is done through the automated measurement and comparison of distinguishing physiological or behavioural traits (UK Biometrics Working Group 2002). The most common forms of biometric identification at present are fingerprint recognition, hand geometry, iris recognition, facial recognition, voice recognition and signature recognition. There are also a number of less common forms of biometric identification, such as gait recognition, keystroke pattern recognition, retina recognition and vein recognition. Almost any part of the body, or any behavioural characteristic, could potentially be used as the basis for biometric identification, although the accuracy and reliability of the procedure will vary.

Any time there is a need for a person to be identified, or to have their identity verified, it is possible to use biometrics. Some of the common areas in which biometrics have been used to date include:

Criminal ID: The use of biometric technologies to identify or verify the identity of a suspect, detainee, or individual in a Law Enforcement application.

Retail/ATM/Point of Sale: The use of biometrics to identify or verify the identity of individuals conducting in-person transactions for goods or services.

eCommerce/Telephony: The use of biometrics to identify or verify the identity of individuals conducting remote transactions for goods or services.

PC/Network Access: The use of biometrics to identify or verify the identity of individuals accessing PCs, PDAs, networks, applications, and other PC-oriented resources.

> Physical Access/Time and Attendance: The use of biometrics to identify or verify the identity of individuals entering or leaving an area, typically a building or room, at a given time.
>
> Civil ID: The use of biometrics to identify or verify the identity of individuals in their interaction with government agencies for the purposes of ID issuance, background checks, voting, immigration, or social services.
>
> Surveillance and Screening: The use of biometrics to identify individuals present in a given space (International Biometric Group 2003, p.90).

The following sections examine briefly the use of biometric systems for authenticating identity. The performance of such systems is discussed first, followed by an examination of biometric standards and biometrics and privacy.

Performance of biometric systems

Biometrics is currently attracting great interest for the apparently higher level of integrity that it offers in comparison to the standard knowledge-based and token-based systems. This is because biometric systems are based on an individual's unique physiological or behavioural characteristics, rather than a token that can be separated from the individual or a piece of information that can be learnt. Due to this physical link between a biometric identifier and a particular individual, biometric systems are seen to be both more accurate and more difficult to fool than other methods of identification.

It should be noted, however, that although potentially more accurate than knowledge-based or token systems, biometric identification systems are not infallible. In fact a number of problems can arise when biometric technologies are used. These include:

- Matching errors: A biometric system may mistakenly match an impostor's biometric to that of a genuine user (a 'false match'). Alternatively, a system could mistakenly fail to match a genuine user's biometric to one previously provided by that same user (a 'false non-match').[147]
- Decision errors: A biometric system may mistakenly accept an impostor to be a genuine user (a 'false accept') or reject a genuine user as being an impostor (a 'false reject'). This could either be due to false matching or

147 Matching errors are often measured in terms of a 'false match rate' (FMR) and a 'false non-match rate' (FNMR). The FMR is the expected probability that a sample will be falsely declared to match a single, randomly-selected template of a person other than the user. The FNMR is the expected probability that a sample will be falsely declared not to match a template from the same user providing the sample. (Mansfield & Wayman 2002). These rates are interrelated, and will vary depending on how the system is set up. For example, while a system can be operated in such a way as to reduce the FMR, the FNMR will increase accordingly. Similarly, while the FNMR can be reduced, the FMR will rise concomitantly. The equal error rate (EER) is the point at which the FMR and FNMR are equal.

false non-matching, because the information obtained is not of sufficient quality, or as a result of any other errors in the whole system.[148]

- Image acquisition errors: A biometric system may not be able to acquire the information needed for identifying an individual or verifying their identity. This may occur because there is no biometric data to collect. For example, an individual without hands will not be able to supply fingerprints. Alternatively, while there may be biometric data to collect, it may be impossible to capture. For example, an individual who cannot move their arms may not be able to place their hands onto a hand geometry sensor, or a person may refuse to use such a sensor on religious or hygienic grounds.[149]
- Spoofing: A biometric system may be susceptible to concerted attempts to fool it, known as 'spoofing'. There are three main ways in which a system can be attacked (Thalheim, Krissler & Ziegler 2002). First, it is possible to use an artificial biometric, such as a fake finger, to fool the regular sensor technology of the system. Second, data can be captured as it is input into the sensor, through use of a device such as a sniffer program. This is a device that can be attached to the back of a computer (eg. in the USB port) and which can obtain information as it is input into the computer. The data captured can then be replayed, to fool the system (known as a 'relay attack'). Third, it is possible to attack the database in which the data are stored directly. This will usually need to be done by someone who has administrator rights over the database, although it could be done through an external attack on the database (hacking).

All current biometric systems are susceptible to these problems, to a greater or lesser extent. For example, evaluations of facial and voice recognition systems have often shown them to be quite inaccurate, with high matching and decision error rates being recorded (United States General Accounting Office 2002). Even the performance of the most widely used biometric system – fingerprint recognition – has been found to vary depending on the type of scanner used (Mansfield, Kelly, Chandler & Kane 2001). The precise nature and extent of the problems faced varies depending on the particular system. For example, retina

148 Decision errors are measured in terms of a 'false accept rate' (FAR) and a 'false reject rate' (FRR). These rates refer to the proportion of transactions in which an impostor is either falsely accepted by the system, or a genuine user is falsely rejected by the system (Mansfield & Wayman 2002). The difference between the FAR/FRR and the FMR/FNMR is that the FMR/FNMR refer to a single comparison between the image acquired and a previously captured sample (do they match?), while the FAR/FRR refer to an entire transaction in which the biometric system makes a decision about whether or not to accept a user as being genuine. As with the FMR and FNMR, the FAR and the FRR are variable and interdependent. Systems can be adjusted so that the FAR is reduced, at the expense of increasing the FRR, and vice versa. It should be noted that these terms are not used consistently in the literature, so caution needs to be taken in examining any results of biometric evaluations.

149 Image acquisition errors are measured in two ways: the 'failure to enrol rate' (FTER) is 'the expected proportion of the population for whom the system is unable to generate repeatable templates', and the 'failure to acquire rate' (FTAR) is 'the expected proportion of transactions for which the system is unable to capture or locate an image or signal of sufficient quality' (Mansfield & Wayman 2002, p.6).

recognition is generally considered to be more accurate than hand geometry. This is because the blood vessel pattern on the back of the eye is believed to be unique to each individual and relatively resistant to changes over one's lifetime, whereas the shape of a person's hand is not (Biometix 2003). However, retinal scanners have been found to be quite difficult to use, compared with hand geometry sensors. This is likely to lead to higher image acquisition error rates for retina recognition than for hand geometry.

Even iris recognition, which is generally regarded as the most accurate of the current biometric technologies, has been found to be vulnerable to spoofing. In tests conducted in Germany, it was found that iris recognition systems could be deceived by taking a photograph of the iris, printing it onto photographic paper (to get sufficient quality), cutting out a hole in the location of the pupil (to provide appropriate in-depth aperture of the pupil required by the scanning software), and placing it over the user's eye (Thalheim et al. 2002). While steps can be taken to enhance the security of such systems, no system yet developed has been found to be foolproof.

In addition, errors could occur when a person initially enrols himself or herself into a biometric system because individuals' biometrics do not, by themselves, identify them. 'Biometric systems can only confirm or determine a claimed identity – one established upon system enrolment – as opposed to revealing a "true" identity' (International Biometric Group 2003, p.17).[150] That is, Amanda Black cannot simply provide her fingerprints for enrolment and have the system ascertain that she is Amanda Black. Rather, she would need to provide some independent evidence of identity (such as a driver's licence or birth certificate) at the same time that she initially enrols. From that point on, her biometric will be linked with the identity of Amanda Black, as originally enrolled. In the future, there will no longer be a need for independent evidence of identity to be provided. It is vital, however, that such evidence be provided on the first occasion.

To this end, it is important to ensure that appropriate identification documents are still provided and background checks made prior to enrolment. 'The integrity of a biometric system is only as good as the quality of the enrolment data.' (Dunstone 2003, p.11). If care is not taken in the enrolment phase, it will continue to be possible for a person to defraud the system, defeating the purpose of using biometrics. Moreover, a real danger arises if a person can successfully bind their biometric data to a stolen identity because this will allow them to continue using that false identity for a variety of fraudulent purposes, with little risk of detection. It will generally be accepted that because a person can provide a biometric that matches the assumed identity he or she must be that person. This may have a significant detrimental effect on the person whose identity has been stolen, and can take a long period of time to clear up.

150 This point was also made by Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, 24 June 2003.

The potential danger of using biometric systems was raised during debate on what became the *Electronic Transactions (Victoria) Act 2000*. A Canadian expert and key figure behind similar legislation passed in Ontario explained:

> A biometric should be regarded as a particularly dangerous form of PIN. A PIN, when it is suspected that it has been compromised, needs to be changed. A biometric cannot be changed. Once compromised, it is compromised for all time (Parliamentary Debates, Victoria 2000b, p.1225).

It should also be noted that even if a biometric system is accurate and reliable, and has adequate enrolment procedures in place, it may not actually act to prevent crime. It is possible that the implementation of biometric systems could simply displace crime, rather than reduce it. That is, a motivated offender who is thwarted by the deployment of such a system may either change tactics in order to get around the system, or change the nature of the crime committed (see, for example, Smith, Wolanin & Worthington 2003). One particular risk of the use of biometric systems is a possible increase in extortion or violent crime. For example, people wishing to defraud the system may seek to force individuals to provide their biometric characteristic on demand by threatening or blackmailing them. Alternatively, a person who wishes to spoof a fingerprint scanner may cut off the finger of the person they wish to imitate, or remove their eye to fool an iris scanner. While such attempts are unlikely to succeed due to technological measures that can detect the 'liveness' of a sample, this may not be sufficient to prevent people from attempting such measures.

Unfortunately, it is difficult to assess exactly how accurate and reliable biometric systems are, or how effective they are at preventing fraud. This is because no single test has been developed which can accurately measure each of these issues, across biometric devices, in a uniform way. This has led to a multiplicity of performance measures being adopted, creating great confusion in this area. This was noted by Mansfield and Wayman (2002, p.1), when they stated that 'even a short review of the technical literature on biometric device testing over the last two decades or more reveals a wide variety of conflicting and contradictory testing protocols. Even single organisations have produced multiple tests, each using a different method'.

The main consequence of this is that any evaluation results need to be treated very carefully. The terminology used is likely to vary, and even when the same terms are used they may be used in different ways. The testing procedures vary widely, making it generally impossible to compare different tests in a meaningful way. Often one of the parties conducting a test will have a vested interest in the outcome, which may have influenced the choice of testing procedures. Even if tests are conducted by an independent body, and contain comparable results, these may not focus on the area of most relevance to an organisation.

In an attempt to rectify this problem, the National Physical Laboratory has produced a document for the United Kingdom Biometrics Working Group,

entitled *Best Practices in Testing and Reporting Performance of Biometric Devices* (Mansfield & Wayman 2002). Version 2.01 was released in August 2002. This document is an attempt to develop a standardised framework for evaluations of biometric technologies. While the document is very comprehensive, due to its recent release it has not yet been widely adopted. It is hoped that subsequent evaluations will comply with its recommended procedures and use of terminology.

Biometric standards

Biometrics is a rapidly changing area. New technologies are being developed on a regular basis, as more vendors enter the field. There are now over 150 vendors in the biometrics industry (Biometix 2003). This creates a need for the continuing development and use of standards, to ensure that deployers of biometric technologies are not locked in to either a technology which may become obsolete or an arrangement with a particular vendor that limits the use of emerging technologies.

A number of different standards have already been produced, with more being developed. Many have been led by the National Institute of Standards and Technology (NIST) Biometric Interoperability, Performance and Assurance Working Group, which seeks to advance efficient and compatible biometric technology solutions. This Working Group consists of 85 organisations representing vendors, system developers, end users, universities, government agencies and industry organisations (http://www.itl.nist.gov/div895/isis/bc/bcwg/).

Probably the most important standard in the area is the Biometrics Application Programming Interface (BioAPI), which aims to enable:

- rapid development of applications employing biometrics;
- flexible deployment of biometrics across platforms and operating systems;
- improved ability to exploit price performance advances in biometrics;
- enhanced implementation of multiple biometric alternatives (fingerprint, voice, face, iris, etc) (http://www.bioapi.org/).

In addition to developing the BioAPI architectural standard, NIST and the Biometrics Consortium have also developed a standard data format to be used within the BioAPI (or other) architecture. This data format, known as the Common Biometric Exchange File Format (CBEFF), is intended to be sufficiently generic to be able to handle any type of biometric. Its purpose is 'to promote interoperability of biometric-based application programs and systems as well as to facilitate biometric data interchange between systems and vendors' (http://www.nist.gov/cbeff).

Other developments in the area include:

- AAMVA: The American Association for Motor Vehicle Administration (AAMVA) has created a standard format for fingerprinting data that provides a uniform means for identifying issuers and holders of drivers' licences in the US and Canada (United States General Accounting Office 2002).
- ANSI X9.84-2000: This standard looks at security requirements for the management of biometrics information in the financial services industry. Although it was developed specifically in relation to the financial services industry, a wider application has been suggested.
- BAPI: Microsoft and I/O Software Inc have announced they will enable biometric technologies to be integrated into future versions of the Microsoft Windows operating systems. Microsoft has developed its own biometric application programming interface, known as BAPI, rather than using the widely accepted BioAPI standard.
- JPEG: The Joint Photographic Experts Group (JPEG) have developed a standard that could be used in facial recognition systems.
- WSQ: Wavelet Scalar Quantization (WSQ) gray-scale fingerprint image compression algorithm is now the standard for exchanging fingerprint images within the criminal justice community (United States General Accounting Office 2002).
- XML Common Biometric Format (XCBF): OASIS, an e-business standards consortium, are developing standards for the way in which biometric applications are coded in XML (Extensible Markup Language), which will affect the use of biometric identification over the Internet (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf).

It can be seen that there are currently a wide range of standards in this area. This is not all due to the existence of conflicting or competing standards. Some of these standards operate in relation to different aspects of biometric systems. For example, the WSQ standard is about standardising the way images are acquired, whereas ANSI X9.84-2000 relates to the way data are transported. It is necessary to have standards in both of these areas. Some of the standards, however, are competing for dominance in the area. In particular, the BioAPI and BAPI standards both relate to hardware and software interfacing. It will ultimately be necessary for one of these standards to gain industry-wide acceptance if true interoperability is to occur.

Biometrics and privacy

The use of biometric systems also raises potential problems in terms of privacy and confidentiality of the personal data stored on computer networks. While some people claim that biometrics can be a privacy enhancing technology

(Biometrics Institute 2002),[151] there is a general perception that the use of such technologies is likely to be privacy invasive. Some of the main privacy concerns include fears that biometric information will be gathered without permission or knowledge, or without explicitly defined purpose; used for a variety of purposes other than those for which it was originally acquired ('function creep'); shared without explicit permission; or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control (United States General Accounting Office 2002). These risks will vary according to the technology that is used, as well as the context in which it is used.[152]

It is possible to take steps to alleviate some of these privacy-related concerns. For example, when the Ontario government was considering the implementation of biometric technologies to prevent welfare fraud it consulted with the Information and Privacy Commissioner Ontario and included the following privacy protective provisions in its *Social Assistance Reform Act*:

- Any biometric information collected under the Act must be encrypted;
- The encrypted biometric cannot be used as a unique identifier, capable of facilitating linkages to other biometric information or other databases;
- The original biometric must be destroyed after the encryption process;
- The encrypted biometric information only can be stored or transmitted in encrypted form, then destroyed in a prescribed manner; and
- No program information is to be retained with the encrypted biometric information. (Cavoukian 1999, p.5).

The Act also specified that neither the director nor an administrator shall implement a system that can reconstruct or retain the original biometric sample from encrypted biometric information, or that can compare it to a copy or reproduction of biometric information not obtained directly from the individual.

In the Australian context, the Biometrics Institute, with some funding from the National Office of the Information Economy, is currently working on the development of a Privacy Code of Conduct. A draft has recently been released for public consultation.

151 Mr Clive Summerfield, Manager for Government Services, VeCommerce, in conversation with the Committee, 24 June 2003, also noted that biometrics can, in some circumstances, enhance privacy. He noted that under some knowledge-based systems there is a need, for example, for call centre operators to have access to the personal information which is used as the basis for identity verification. This raises the danger that that personal information could be obtained and used fraudulently by those call centre operators, to perpetrate identity-related fraud. Mr Summerfield argued that biometrics could prevent such a possibility, because there would no longer be a need for such personal information to be stored in the system.

152 A comprehensive guide to privacy and biometrics can be found in the Federal Privacy Commissioner's paper 'Biometrics and privacy: The end of the world as we know it or the white knight of privacy?' (Crompton 2002).

The Committee's position on biometrics

Until additional, large-scale, independent testing is carried out, the Committee is reticent to recommend the widespread implementation of biometric systems, particularly across the public sector. The Committee is concerned that the weaknesses of such systems are understated by many biometric advocates who seek to present the implementation of such systems as being a panacea to prevent all fraud. As noted in the brief discussion above, such systems are not infallible, and the accuracy and reliability of many systems is highly questionable. The Committee believes that until these issues are resolved there is a danger in using biometric systems of engendering a false sense of security, which actually may be more damaging than helpful. Accordingly, the Committee does not recommend the implementation of such systems until their accuracy is improved.

The Committee does, however, encourage the development of standards governing the use of biometrics. The Committee also believes that it is vitally important to take measures to protect people's privacy prior to the wide-scale implementation of biometric systems. Such measures are not only important in addressing the concerns outlined above but also in encouraging user acceptance of biometrics, which will be necessary if they are ever to be successfully deployed (Mansfield & Wayman 2002). To this end, the Committee encourages the development of a Privacy Code of Conduct. The Committee further recommends that biometric-specific privacy protections be incorporated into legislation before such systems come into widespread use.

Recommendation

17. The Committee recommends that biometric systems not be widely implemented by the Victorian Public Service for fraud control purposes until the technology is more accurate and reliable, appropriate standards have been developed, and biometric-specific privacy protections have been incorporated into legislation.

Smart cards

As discussed in Chapter 4, one technological approach to the prevention of some forms of plastic card fraud is the use of so-called 'smart cards' or cards with silicone chips embedded in the plastic. As discussed, card skimming is a continuing problem for the financial services industry, with data contained in the magnetic stripe of the card being relatively easy to copy and reproduce on a blank counterfeit card. In order to overcome this problem, plastic card data can be contained in a computer chip that is securely embedded in the plastic card structure. This enables the card to be authenticated, the cardholder verified, exception files to be checked for compromised cards, and floor limits to be complied with where independent authentication checks are required. Data are encrypted making it almost impossible to compromise the security of the card.

From the user's perspective, the use of chip cards would mean that they would never be liable for unauthorised transactions carried out in accordance with the issuer's rules of usage. In addition, it is possible to change the parameters on the card without having to re-issue the card, and chip cards are more robust and tamper-proof than magnetic stripe cards (New 2003).

Chip cards are now being used in conjunction with PINs which further limits opportunities for lost or stolen cards to be misused, unless, of course, the PIN is carried with the card (contrary to the instructions of card issuers). The implementation of chip and PIN, however, requires the extensive roll-out of card readers at every point of sale and ATM. In Australia, for example, there were 20,899 ATM terminals and 446,111 EFTPOS terminals as at September 2003,[153] each of which would need to be replaced or adapted to make them suitable for chip cards and PIN readers. Currently chip cards cost between US$0.99 and US$2.00 depending on capabilities, and the average cost of converting terminals is approximately US$200. It is likely that chip cards used in conjunction with PIN will be fully implemented in Australia by the end of 2008 (New 2003).

Chip cards with PIN readers have already been implemented in a number of countries. In France, Malaysia and Switzerland, chip cards are being used for domestic transactions (New 2003). In Britain in 2002, card issuers and acquirers continued to upgrade the card payments infrastructure to chip technology with more than 41 million chip cards in issue at the end of the year, around 430,000 chip terminals deployed at point-of-sale and more than 25,000 cash machines equipped with chip readers. It is anticipated that by 2005 the vast majority of card-based transactions will use chip cards and PIN authentication. The initial trial of chip cards used in conjunction with PINs in Britain commenced in May 2003 in Northampton adopting the global standard specification that was set by the international card schemes Europay, MasterCard and Visa (EMV) (Association for Payment Clearing Services 2003).[154]

Chip cards do not, of course, solve all plastic card fraud problems, as card-not-present fraud, such as that carried out in online transactions, will continue to occur. Other strategies such as the use of Card Verification Numbers (CVN) and Address Verification Services (AVS) have been designed to minimise card-not-present fraud. In particular, CV2 (Card Validation Code 2) has been extremely effective in reducing card-not-present fraud. When making orders, customers are required to quote the last three digits of the 16 numbers on the back of the card which are unique to each card. This ensures that the cardholder is in actual possession of a card and not merely using numbers which could have been obtained without authorisation. A study by Visa International found an 84 per cent reduction in payment denied losses and a 57 per cent reduction in chargebacks when CV2 was used, with potential to reduce losses from $7.5

153 http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Stats_Terminals.

154 See http://www.chipandpin.co.uk.

million to $2 million and dispute handling costs by $2.7 million a year (McKindley 2003).

Recommendation

18. The Committee recommends that the Victorian government should support the early roll-out of EMV standard computer-chip plastic cards for use in electronic transactions in conjunction with Personal Identification Number (PIN) authentication.

Secure online transactions

The development of the Internet and electronic commerce has resulted in a large increase in card-not-present fraud. This takes place when customers disclose credit card account numbers and card expiry dates when placing orders online and offenders make use of this information to order goods and services illegally. Online transactions, of course, contain the same risk elements as telephone orders and mail orders where cards are not physically seen by merchants. To counter these risks, card issuers in conjunction with computer hardware manufacturers and software developers have been considering the use of secure systems to facilitate online transactions for a number of years.[155]

In order to enhance the security of credit card transactions on the Internet, various companies have designed systems to ensure that the identity of the contracting parties can be authenticated and that merchants can ascertain if the customer has adequate funds with which to conduct the transaction. Various protocols have been developed beginning with the Secure Electronic Transaction (SET) protocol created by Visa International and Mastercard Limited in the mid-1990s and then moving to the three Domain Model, the Universal Cardholder Authentication Field (UCAF) and, most recently, the 3D Secure Visa protocol (Verified by Visa). After a Visa cardholder enters his or her card number on the web site's payment page, the Merchant Plug-In on the computer connects with the Visa Card Issuer to check if the card is secured with Verified by Visa. The card issuer then initiates a Verified by Visa pop-up window on the cardholder's computer screen, the customer enters a password, and the card issuer can confirm the cardholder's identity back to the merchant. The transaction can then proceed normally.[156]

Mastercard has developed corresponding systems including SPA Secure Code (for Australia), 3D Secure Code, and CAW (Kwakernaak 2003).[157] Within five years it is likely that all Visa and Mastercard transactions that take place online will employ Verified by Visa or Mastercard Secure Code systems (McKindley

155 Submission from Mr Glenn Bowles, Director, bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

156 http://www.visa.com.au/verified/index.shtml.

157 http://www.mastercard.com/securecode/sc_newbie.html.

2003). These systems check if cards have been enrolled in a directory and then correlate cardholder details with the card issuer. Authentication and authorisation are thus separated with user authentication carried out through the use of an encrypted PIN that is not known to the merchant or other parties. Systems are designed to be easy to use with the customer simply providing the card number and using the secure number.

Although these systems minimise many of the key risks associated with card-based transactions where the card is not actually present, they still require users to enrol and, accordingly, to produce evidence of identity. Many of the same problems that confront the use of the 100-point system also apply in this context as offenders could obtain secure transaction codes in another person's name or make use of other users' secure codes. As a result the risks are merely shifted further back.

In the public sector the principal developments have involved the creation and implementation of *Gatekeeper* which is now accepted as 'the gold standard' for securing transactions with and between large government agencies.[158] The implementation of Gatekeeper was explained to the Committee as follows:

> Gatekeeper is basically an accreditation system based on a set of standards. The federal government has decided that individual Commonwealth agencies must make a decision about what kind of authentication system they should use. The agency decides that if they decide they are going to use PKI – and only a small number have to date – then they must use Gatekeeper-accredited service providers, and NOIE coordinates the accreditation process, which is somewhat time-consuming, somewhat complex and is not cheap, but the reason for that is that you are actually trying to come up with something in which you can have very high levels of trust. For simpler transactions, things like PIN and password combinations are probably entirely appropriate.[159]

To date, however, the implementation of public key systems has been relatively slow around the world, with some limited exceptions. These include Hong Kong, where the Customs Authority has about 300,000 digital certificates in use every day, and the United States, where a number of government agencies are undertaking a large-scale roll-out of PKI. In Australia, the only significant roll-out has been undertaken by the Australian Taxation Office (ATO), which has issued about 120,000 digital certificates, of which 70,000 are in routine use. The ATO is also in the process of conducting an even larger roll-out of Australia Business Number-Digital Signature Certificates (ABN-DSC), which will be a common certificate that can be used across a number of different groups, rather than a single-use certificate like most digital certificates currently existing in Australia.[160]

158 Mr Keith Besgrove, Chief General Manager, Regulation & Analysis Group, National Office for Information Economy, in conversation with the Committee, Canberra, 24 June 2003.

159 Ibid.

160 Ibid.

What is required now is for the various states and territories to implement *Gatekeeper* for their own secure online transactions. A representative of Standards Australia told the Committee that a proposal has been put to the National Office for the Information Economy as to how this could best be achieved.[161]

The problem remains, however, that private key data or tokens for use in public key systems or secure code transactions must themselves be communicated to users and customers. The financial world has already experienced considerable problems in transferring possession of plastic payment cards to users and similar problems could arise with respect to cryptographic keys that are stored on smart cards. Security precautions would be needed to ensure that tokens are passed securely to users from the issuing authority (see the discussion of this issue in Office of Government Information Technology 1998).

Another area of risk concerns the generation of cryptographic keys and secure codes (Office of Government Information Technology 1998). It may be possible for the individual who generates a public and private key pair to retain a copy of the private key for later illegal use. Legislation is needed to proscribe conduct of this nature. Cryptographic keys would be kept on the hard drive of a computer with the cryptographic service activated by a smart card inserted into the personal computer. Smart cards may also be used to sign a digital signature and to authenticate the identity of a user. In addition to the risks associated with compromising access to mechanisms such as PINs, passwords and biometric devices, the possibility exists that smart card tokens themselves may be altered or counterfeited. Already this has taken place in relation to smart cards used for small-value commercial transactions. Where keys are stored on personal computers or servers, their security may be compromised, in which case appropriate risk management measures must be taken.

An example of the risks associated with the use of encrypted authentication systems arose recently when the Microsoft product VeriSign was tricked into issuing false digital certificates in Microsoft's name (Bader 2001; Markoff 2001). The certificates in question were not used for electronic commerce transactions, but for checking the authenticity of the name of the developer of software programs. The problem that arose in the human verification part of the process of issuing digital certificates could also occur in electronic commerce authentication procedures. The main lesson here appears to be that no technology can of itself be relied on to provide security. The foibles of a system, the points susceptible to fraudulent human interception – wherever they may be, for they are always present – must be known and vigilantly guarded.

161 Mr Mark Bezzina, Director, Communications, IT and eCommerce, Standards Australia, in conversation with the Committee, Sydney, 25 June 2003.

Recommendations

19a. The Committee recommends the adoption of the proposals set out in the *Gatekeeper Strategy* concerning secure electronic transactions, and supports the adoption of the *Gatekeeper*-compliant framework at a state level .

19b. The Committee recommends that Registration Authorities which issue public-private key pairs for use in secure electronic transactions be required to adopt the same standards for identification of users as are required to open an account with a financial institution under the Financial Transaction Reports Regulations 1990 (Cth).

19c. The Committee recommends that legislation be passed making it illegal to generate and retain a copy of a private key without consent, once the original has been passed on.

Pre-employment screening

As discussed above, organisations that do not attempt to verify the identity of new clients run a risk of being defrauded. Similar risks apply to employers who do not seek to verify the identity and credentials of those whom they intend to employ, whether at the level of junior staff or senior management. These risks range from employing someone with fraudulent credentials who may be unable to perform their job adequately, to the more serious risk of employing a person with a history of fraudulent behaviour who may defraud his or her new employer as well. As demonstrated in previous surveys (see Chapter 3), the higher the level of employment, the greater the risk of financial fraud occurring. KPMG found in its survey of 361 of Australia and New Zealand's largest public and private sector organisations that the average loss per organisation through fraud perpetrated by internal managers was $434,664, while the average loss through fraud perpetrated by non-managerial employees was only $132,277 (KPMG 2002). Similarly, in Ernst & Young's *8th Global Fraud Survey*, some 55 per cent of perpetrators of fraud were managers and 85 per cent of managers committing the largest frauds had spent less than a year in that managerial position (Ernst & Young 2003).

The risk of re-offending is seen to be quite strong. For example, in evidence given to the Committee in relation to a study of fraud in the financial services sector, it was noted that:

> The one thing that really did come through was that a quite surprising amount were believed to have committed fraud before. Now obviously the firms that were involved in this didn't know about it before they took the people on, but after they discovered this person had committed fraud, in a number of cases they said, look, we found out that there was a strong suspicion they had done it somewhere else or they had done it elsewhere… and they were currently going through the courts or the investigation process when they joined… So,

> certainly, one of the issues is … the strong sense we have got [that] people who have done this once are quite likely to do it again…[162]

To address this risk, it has been suggested to the Committee that greater use should be made of pre-employment screening.[163] In particular, it has been suggested that prospective employers should confirm that the applicant is really who they say they are and have done what they say they have done. This might involve calling past employers, referees, universities where they have obtained degrees, or seeking other forms of confirmation of their history and provenance, including criminal background checks. In interviews, links should be sought between this information and the prospective employee, through photographic identification, or even, it was suggested, through biometrics.[164] Mr Ringin of Pro Active Strategies Pty Ltd commented that:

> There is a draft Australian standard currently on the books which says that a thorough pre-employment screening process is considered by some experts to be the most effective way of minimising and guarding against potential security risks by identifying undesirable employees before they join an organisation.[165]

Although pre-employment screening is already used by many organisations,[166] many others do not make any such checks. The need for such screening can be seen in the results of a survey of the backgrounds of Internet company managers conducted by Kroll between June and August 2000. The global survey of 70 Internet corporations found that executives in this sector were four times as likely to have 'unsavoury' backgrounds as executives from other industries. The 20 respondents from Internet corporations in Asia, Australia and New Zealand were particularly likely to have executives with questionable histories – including individuals who had allegedly been arms dealers, convicted criminals, smugglers and thieves. One Internet company hired a suspected arms dealer to run its operations across two Asian countries. Two Internet companies in the region were found to have had links with organised crime (Needham 2000). Although these allegations may be difficult to verify, they do raise the problem of Internet companies sometimes failing to have adequate internal controls and procedures in place to screen staff when recruiting.

162 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

163 Mr Shane Ringin, Pro Active Strategies Pty Ltd, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

164 Mr Shane Ringin, Pro Active Strategies Pty Ltd, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

165 Ibid.

166 For example, Mr Andrew Tuohy noted that KPMG Forensic conduct criminal checks and background checks on new employees (with their consent), and ensure university accreditations are correct (Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003).

Standards Australia has recently addressed this issue in AS 8001-2003 *Fraud and Corruption Control*, in which it was noted that:

> Many employees who are committing fraud against their employer are found subsequently to have had a history of dishonesty with previous employers.
>
> Entities should conduct pre-employment screening for all new employees appropriate to their position description in order to gain a reasonable understanding of the candidate's employment history and in order to make an informed decision as to whether any prior history of illegal or unacceptable behaviour is compatible with the proposed position to which they are to be appointed (Standards Australia 2003b, p.17).

Standards Australia (2003b) has recommended that the following steps be taken (with the express permission of the prospective employee) to confirm an individual's prior history:

- Verifying the prospective employee's identity (by viewing a birth certificate or driver's licence);
- Checking their police criminal history;
- Conducting a reference check with the two most recent employers, usually by telephone;
- Considering any gaps in employment history and the reasons for those gaps; and
- Verifying any formal qualification claimed.

The Committee recommends that VFIRC should promote the use of such measures to screen personnel prior to employment in the public and private sectors, so as to to assist in the detection of individuals who might be at risk of behaving dishonestly. The Committee is concerned to ensure, however, that such checks are only conducted with the express permission of the prospective employee, to protect his or her privacy.

The Committee notes that a number of parties raised concerns about the unwillingness of previous employers to tell prospective employers about suspected but unproven acts of dishonesty.[167] Such an unwillingness may arise due to a fear of being sued. For example, advising of such allegations may breach the duty of care owed by previous employers to their employees when giving a reference, giving rise to a claim of negligence (see, for example, *Spring* v *Guardian Assurance* [1994] IRLR 460; *Cox* v *Sun Alliance Life Limited* [2001] IRLR 448). It could also potentially give rise to claims in defamation, injurious

167 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003; Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dennis Challinger, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

falsehood, unlawful discrimination or victimisation, or misleading and deceptive conduct under the *Trade Practices Act 1974* (Cth) (Holding Redlich 2002).

Due to the possibility of such suits being brought against them, previous employers may choose not to provide a reference or information about the suspected acts of dishonesty.[168] This makes it difficult for prospective employers to assess the trustworthiness of their new employee, and impacts on their ability to minimise the risks of fraud. While the Committee would prefer that employers could be frank and honest about any dishonest behaviour perpetrated by employees, this raises issues beyond the scope of the current Inquiry. The Committee cannot, therefore, make any recommendations in this area.

Recommendation

20. The Committee recommends that VFIRC should promote the use in the public and private sectors of effective measures to screen personnel prior to employment, to assist in the detection of individuals who might be at risk of behaving dishonestly.

Risk management strategy and guidelines

It can be seen from the discussion above that there are a variety of different procedures and technological solutions that have been devised to address the problems associated with user identification. Each of these measures has its own strengths and weaknesses. For example, the use of passwords may be relatively cheap, but also fairly insecure. By contrast, the use of biometric authentication systems may offer an additional sense of security, but at greater expense and with a possible loss of user friendliness.

Given the range of options available, it is important for all organisations to carefully consider their specific needs in determining which kind of system is most appropriate. The Committee is in agreement with the National Office for the Information Economy (2002, p.15) that 'the approach adopted should be determined by the outcome of a risk assessment and subject to the preparation of an associated business case. [Organisations] should also consider the needs and expectations of their customers.'

In its publication *Online Authentication*, the National Office for the Information Economy sets out some of the factors to consider when deciding on an appropriate online authentication system. This includes the level of risk involved if proper authentication systems are not in place, and the likely costs

168 It should be noted that if an employer does provide a reference, a duty of care is also owed to the person to whom the reference is provided (*Bartholomew* v *London Borough of Hackney* [1999] IRLR 246). So if a previous employee has been dismissed for fraudulent behaviour, and the employer provides a reference claiming they were an honest employee, and they are employed and steal from their new workplace, the new employer can sue the original employer for having made a negligent misstatement that caused economic loss.

associated with a failure to properly authenticate parties, as well as the different authentication options available to address those risks, their benefits and weaknesses, and the costs of implementation. The Committee recommends that VFIRC develop a similar guide to aid Victorian organisations determine the appropriate authentication systems to be used, but that it be expanded to include all forms of authentication, not just online authentication (see Recommendation 22b). This guide could be used by public sector entities to determine an appropriate authentication strategy when they draft their fraud control and information security management policies (see Recommendations 6a and 11a).

Web certification services

Finally, online consumers can be assisted in making choices about whether or not to engage in electronic commerce transaction by relying on various web seals that are placed on some Internet sites. For a number of years now, organisations have been providing certification services to enable users to identify legal, safe Internet sites. Users are then free to decide whether or not they wish to make use of the material in question and whether or not to conduct transactions with the online merchant. (See, for example, the 'Which' webtrader site, http://whichwebtrader.which.net/webtrader/.)

The Council of Better Business Bureaus in the United States, for example, carries out a certification service in which Internet business sites are given a form of approval. Sites that agree to abide by the Council's truth-in-advertising standards and to adopt its dispute resolution procedures may display the authorised and encrypted seal of approval. Members of approved Internet associations are able to display the fact of their membership and consumers are able to check to see if organisations have membership.

The WebTrust program, developed by the American Institute of Certified Professional Accountants, certifies Internet sites which demonstrate sound online business practices after having undergone an extensive auditing procedure (AICPA 2000). The audit, which varies in cost depending upon the complexity of the business and the site, includes the site's security measures, privacy practices and transaction-processing systems.

The service is available from any WebTrust-licensed Certified Professional Accountant or accounting company. Since the AICPA began the WebTrust program, some 1,500 Certified Professional Accountants and 75 accounting companies have qualified to perform WebTrust audits (Tweney 1998). To date, only a small number of sites have passed the audit, permitting them to display the WebTrust seal. Like other third-party certification programs, WebTrust depends for its success on widespread acceptance by online merchants and, more importantly, by users, both of which, it is to be hoped, will be achieved over time.

In Australia, a few organisations have established certification services of varying degrees of sophistication, although these are less extensive in coverage than the more established models in the United States and the United Kingdom.

In January 2002, Consumer Affairs Victoria (2002b) released a Discussion Paper on web seals which described some common seals, noted the consumer issues which they raised and suggested options for government action. The Discussion Paper was circulated to the Standing Committee of Officials of Consumer Affairs in May and July 2002, and in August 2002 the Ministerial Council on Consumer Affairs agreed to the inclusion of web seals of approval on its strategic Agenda and asked the E-commerce Working Party to give further consideration to the issue.

In September 2003, Consumer Affairs Victoria (2003) released an 'Options Paper' which examined comprehensively the whole question of certification services and web seals. The paper suggested that there may be too many web seals and that the standards under-pinning them were not fully transparent. As a result, it was suggested that consumers have no way of assessing the value of seals of approval, which accordingly detracts from their usefulness. The options canvassed in the paper include developing a Guide to Web Seals, developing criteria for effective seal schemes and establishing a national seal accreditation body similar to TrustUK in the United Kingdom.

Certification and endorsement services can offer significant benefits and help to regularise electronic commerce. The fact that a business is certified gives individuals some measure of confidence in the trustworthiness of that business and in the availability of redress mechanisms if problems arise. To support this trend, providers of payment facilities could be encouraged to deal only with certified businesses who have agreed to comply with a code of conduct which meets certain minimum standards. This would provide a powerful industry-based inducement for businesses to undergo certification and to act in conformity with established codes of practice.

As the Consumer Affairs Victoria 'Options Paper' noted, one of the main problems with endorsement and certification is the proliferation of services and the determination of appropriate standards. Determining acceptable standards and publicising these will represent a major challenge for the future. In KPMG's *Global eFraud Survey*, only 12 per cent of respondents stated that their web site had a seal identifying that their system had passed a security audit. Similar percentages were evident for all countries except Australia and the United Kingdom, where only 2 per cent of respondents reported having seals in place. This low level of usage of seals was said to be due to security audits not being well known or understood, or not being regarded as being an effective security measure (KPMG 2001).

An issue of concern is whether web seals could be used by businesses that do not meet appropriate standards. Digital technologies make it easy to copy a seal or logo and it would then be necessary for users to visit the appropriate certification authority to ensure that the seal has been legitimately affixed. Arguably, many consumers would be reluctant to carry out such further research, possibly seeing this as unnecessary or leading to unacceptable delays. The Committee believes that appropriate technologies should be developed to ensure that web seals cannot be counterfeited and also that a quick and efficient mechanism be provided for users to verify the authenticity of seals. The question of creating criminal offences for individuals or entities that apply a web seal to their Internet site without appropriate authority should also be considered. Generally, however, the Committee is supportive of the notion of web seals as long as they meet appropriate standards of accreditation, and suggests that the question be further investigated. One option would be for VFIRC to be the responsible accreditation agency for web seals used by businesses and organisations throughout Victoria.

Recommendations

21a. The Committee recommends that VFIRC establish and maintain a system for the accreditation of web seals that comply with accepted standards concerning content and honesty, and that this system be promoted for use by all Victorian online trading organisations.

21b. The Committee recommends that consideration be given to creating a criminal offence for an individual or corporation to apply a web seal to an Internet site without appropriate authorisation from the accrediting agency.

Conclusion

This chapter has examined a number of different technological and procedural steps that can be taken to help minimise fraud. Such measures will become increasingly important as businesses and government agencies make greater use of electronic commerce and electronic procurement, where the need to authenticate users' identities is of critical importance. The use of such measures, in conjunction with the fraud prevention policies discussed in Chapter 5, can help build a general fraud control framework aimed at addressing the growing problem of fraud, particularly identity-related fraud. Such a framework is seen to be necessary in light of the inability of law enforcement agencies to tackle this problem on their own. This was noted by Mr Alastair MacGibbon, the Director of the Australian High Tech Crime Centre, when he advised the Committee that:

> [W]e cannot be all places and all things to [all people]. That is why we also encourage them to raise their own defences, to have the right virus software, to have the right firewalls and the right policies and procedures in place, the

> right response through forensic guides or through the retention of data through the IIA Code, to try to harden the target and make it better when they do have an incident.[169]

While such policies and procedures are of the utmost importance, their full benefit will only be achieved if people are aware of their existence and take steps to ensure they are properly implemented. The dissemination of fraud-related information is the focus of Chapter 7.

169 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

7. Information Services and Registers

Introduction

It is clear from the submissions and evidence to the Committee that 'fraud prevention involves more than merely compiling carefully designed fraud control policies'.[170] While such policies are essential, education too is a key fraud control measure. Management and staff of organisations need to be educated about the risks of fraud and about prevention measures. Members of the community also need to be educated about the fraud-related risks they face and steps they can take to minimise those risks. This chapter focuses on how this information can be provided. It begins by examining the provision of information generally, then looks at proposals for establishing specific registers to guard against dishonest practices.

Information services

Throughout this Inquiry the Committee has found that fraud is constantly evolving. Not only is the incidence of fraud increasing, but the ways in which it can be perpetrated are also changing, particularly due to the development of computing and communications technologies. This creates a need for continued education. If individuals and organisations are to take effective steps to prevent fraud, they must first be made aware of the potential risks they face and the measures that can be taken to prevent those risks occurring.

There are numerous ways in which such information can be obtained. For example, large public sector agencies that face a constant risk of fraud, and which may have whole departments dedicated to fraud prevention, may be able to obtain relevant information from other agencies working in the area. This is the technique used by the Australian Taxation Office, as noted by the Assistant Commissioner: '[F]raud is not static… it is evolving, and there is a fair amount of interaction between various parts of the ATO and also with other government agencies to make sure we are addressing things'.[171]

---

170 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

171 Mr Rory Mulligan, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

One of the submissions received by the Committee noted that information sharing has been assisted in the United States by the development of Information Sharing and Analysis Centres (ISACs). These Centres have been introduced in the areas of banking and finance, telecommunications, power, water and homeland defence to facilitate intelligence gathering and sharing between finance and banking, law enforcement, government and regulatory agencies.[172]

Smaller organisations, or concerned individuals, may not have access to such sources of information. Instead, they may need to rely on publicly accessible information, such as that provided by law enforcement agencies, regulatory agencies or other bodies working in the area. Such information is widely available on the Internet. A variety of organisations, both internationally and within Australia, maintain web sites aimed at informing organisations and individuals of the risks of fraud, and the steps which can be taken to prevent it.

In particular, there are a number of web sites aimed at reducing the risks of Internet and electronic commerce-related fraud. These include Internet Fraud Watch (http://www.fraud.org/internet/intset.htm), Cyberangels (http://www.cyberangels.org/) and the ScamBusters e-Zine (http://www.scambusters.org/). The Merchant Risk Council web site contains a simple 'Fraud Test' aimed at helping businesses to ascertain how vulnerable they are to the risks of fraud, and some steps that can be taken to help prevent such risks (http://www.merchantriskcouncil.org/fraud.php). The main question, 'How vulnerable are you to fraud?' is broken down into the following series of questions, with a yes/no/don't know response choice:

- Does your web site have a firewall?
- Do you employ effective data security and hiring practices?
- Do you avoid storing card account numbers on a server connected to the Internet?
- Have you installed the latest fraud detection software?
- Do you default to the highest SSL (secure sockets layer) encryption that a consumer's browser can support?
- Do you keep informed about the latest fraud trends and news?
- Do you know what law enforcement agency to contact if your business is victimised by fraud?
- Do you take advantage of card companies' address verification systems? (http://www.merchantriskcouncil.org/fraud.php)

Practical advice on security and privacy protection for Internet purchases is also available from the Internet Fraud Complaint Center (2001a) on the following topics:

- Internet auction fraud;

172 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

- non-delivery of merchandise;
- credit card fraud;
- investment fraud;
- Nigerian letter scams; and
- business fraud.

In another international initiative in the area of consumer-related Internet fraud, a multi-lingual web site (http://www.econsumer.gov) has been established to provide information on consumer protection legislation and other online fraud prevention measures. This site also has a co-ordinated complaints mechanism.[173] Countries participating are Australia, Belgium, Canada, Denmark, Finland, Hungary, Latvia, Mexico, New Zealand, Norway, Sweden, Switzerland, the United Kingdom and the United States. The scheme is maintained by the Federal Trade Commission in the United States and is supported by consumer affairs organisations in each country, the International Marketing Supervision Network, the Consumer Sentinel Network and the Organisation for Economic Cooperation and Development.

An Australian web site (http://www.scamwatch.gov.au) was launched by consumer affairs agencies around the country in October 2001, to educate consumers about online fraud risks. The consumer affairs agencies, including the (federal) Australian Competition and Consumer Commission (http://www.accc.gov.au) and the Office of Consumer and Business Affairs Victoria (http://www.consumer.vic.gov.au), also offer their own resources on the issue. Other Australian-based web sites that provide fraud-related advice and information include:

- Consumers Online (http://www.consumersonline.gov.au), a Commonwealth 'one stop shop for consumer information' run under the auspices of the Department of Treasury, which also maintains a guide to best practice and international developments in electronic commerce (http://www.ecommerce.treasury.gov.au);
- The National Office for the Information Economy (http://www.noie.gov.au);
- The Office of the Federal Privacy Commissioner (http://www.privacy.gov.au); and
- The Australian Securities and Investments Commission's consumer watch site FIDO (http://www.fido.asic.gov.au).

The Committee feels that although abundant information is available from these resources, there remains a need to co-ordinate the provision of information. Hence, the Committee's proposal to establish a single

173 Submission from Mr Robert Antich, Australian Competition & Consumer Commission, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 3 October 2003.

organisation that could co-ordinate and disseminate all kinds of fraud prevention information and advice for Victorians. The nature of this proposal is discussed below.

Proposed reforms

It can be seen from the discussion above that there is no dearth of advice being dispensed in relation to fraud prevention matters. If anything, people seeking guidance in the area may suffer from information being disseminated through too many avenues. This can be confusing, particularly given the different ways in which fraud is dealt with in different jurisdictions. In addition, many of these sites focus on specific elements of fraud, such as Internet or electronic commerce-related fraud, rather than providing an overview of fraud in general. This can necessitate visiting a variety of different web sites in order to obtain comprehensive information.

To address this problem, the Committee recommends the establishment of a Victorian Fraud Reporting and Information Centre (VFIRC) that would become the central Victorian agency responsible for providing information to the public and private sectors in relation to fraud prevention matters. VFIRC would be a 'one-stop shop' for all fraud-related matters in Victoria. This role of VFIRC should be widely promoted, so that any organisations or individuals seeking fraud-related information would know that their first step should always be to contact VFIRC.

In undertaking this role, the Committee recommends that VFIRC should develop and maintain a web site containing fraud prevention information for the public and private sectors and for individuals. Such a web site would become a central repository for fraud-related information, containing information about a variety of different fraud risks and steps that can be taken to help minimise those risks. It would also contain links to other bodies working in the area, both in Australia and internationally.

In addition to maintaining this web site, VFIRC would carry out programs designed to inform the business community and individuals in Victoria of the risks of fraud and electronic commerce-related crime, and of the fraud prevention measures that can be used to minimise the risk of victimisation. This would include a mail-out to all Victorian households of an information brochure on prevention methods that can be used to reduce the risk of fraud victimisation in consumer transactions, business transactions, and electronic transactions, highlighting the importance of the responsible maintenance of passwords and PINs (see Chapter 6). The need for such a public awareness campaign, particularly in relation to the risks of online shopping, was brought to the attention of the Committee.

VFIRC should not only develop an information brochure on prevention methods but should also draft best practice guidelines to help organisations create a fraud prevention framework, and work with such organisations to help

implement that framework. In particular, the Committee recommends that VFIRC develop best practice guidelines to help organisations implement authentication systems (including password management systems) appropriate to their security needs.

VFIRC should also conduct training sessions and/or seminars in relation to fraud control (including information security management), to help inform those working in the area of current risks and preventative measures. Regular forums could be held to put forward and discuss ideas and trends, and to identify changing practices in fraud prevention. VFIRC should also encourage public and private sector agencies to disseminate and explain their fraud control policies widely amongst staff and periodically hold their own in-house fraud prevention training where appropriate. Such training is already provided by a number of organisations and is found to be very useful, particularly if delivered in an engaging fashion. For example, the Director of Fraud Prevention and Control at the Australian Taxation Office told the Committee that:

> The Mars organization did a survey on staff understanding of fraud and the ATO, and it was actually quite revealing in that it was quite low. It was a situation where the staff recognition of fraud problems was not that high. We then commissioned ABC television and Wollongong University and another technical company to put together a training program for us that actually looked at delivering a message on integrity ethics and fraud awareness in an interactive and entertaining way… We facilitate delivery around the country to staff, and we actually record the participation so we know people have attended. The national program managers make sure their staff are on the program… We also use our on-line newsletters to promote fraud and ethics awareness. We have engaged Pryor the cartoonist to help us to be entertaining while delivering important messages. So we are trying to be a little bit innovative there… For some of these interactive programs we have received some pretty high acclaim.[174]

Such training would be particularly important for organisations that employ staff in positions where they are required to verify documents used to establish identity. Such organisations should be strongly encouraged to train their staff in identifying counterfeit and altered documents. Similar training should be provided for organisations that accept credit cards as a form of payment, to help merchants identify counterfeit or stolen cards.[175]

174 Mr Peter Zdjelar, Director of Fraud Prevention and Control, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

175 Mr Bruce Cox, Regional Director Global Security, American Express, noted that American Express spends considerable resources training merchants on the security features of cards, what to look for, and what to do if they find a problem. They have Internet sites and training videos to assist in this task, as well as fraud packages. They also provide specialised training for particular industries that are at risk (Mr Bruce Cox, in conversation with the Committee, 25 June 2003).

As noted in Chapter 3, ideally agencies similar to VFIRC would be developed in each state and territory, with each agency becoming the central provider of fraud-related information for that region. Information from each of these agencies could then be sent to a national body, the Australian Fraud Centre (AFC), which would become a central repository for all fraud-related information across the country. This national body could co-ordinate the information provided by each state and maintain its own web site with links to relevant state, territory and federal bodies.

Recommendations

22a. The Committee recommends that VFIRC be the central Victorian agency responsible for providing information to the public and private sectors in relation to fraud prevention matters.

22b. The Committee recommends that, in addition to the activities outlined in the recommendations above, VFIRC conduct the following fraud prevention activities:

i. Carry out programs designed to inform the business community and individuals in Victoria of the risks of fraud and electronic commerce-related crime and of the fraud prevention measures that can be used to minimise the risk of victimisation. This should include a mail-out to all Victorian households of an information brochure on prevention methods that could be used to reduce the risk of fraud victimisation in consumer transactions, business transactions, and electronic transactions, highlighting the importance of the responsible maintenance of passwords and PINs;

ii. Conduct training sessions and/or seminars in relation to fraud control (including information security management), as well as encouraging public and private sector agencies to disseminate and explain their fraud control policies widely amongst staff and periodically hold in-house fraud prevention training. In particular, where staff are required to verify documents used to establish identity, organisations should be encouraged to train them in identifying counterfeit and altered documents;

iii. Develop best practice guidelines to help organisations implement authentication systems (including password management systems) appropriate to their security needs; and

iv. Develop a web site containing fraud prevention information for the public and private sectors and for individuals.

Fraud prevention networks

The Committee also believes an informal forum would be useful, within which fraud-related matters could be discussed by those people who actually deal with

such issues. For example, it would be helpful for those who are developing fraud control policies to be able to discuss the drafting of such policies with others who have been involved in a similar process. While the general provision of information by VFIRC would clearly assist in performing such tasks, being able to discuss with others in the field exactly how recommended measures can be applied in practice would also be of great assistance.

Such a forum already exists in New South Wales with respect to corruption. The Corruption Prevention Network (CPN) provides a mediated email forum through which individuals can discuss any fraud or corruption-related issues. Those with particular questions simply pose such questions to the forum, with other members replying at will. An annual conference is also held, in which recent trends and issues are discussed.

The CPN is not a formal government organisation. It was formed in 1989 by individuals working in the field and is administered by a committee of elected volunteer public officials who are practitioners in corruption prevention. While some seed funding was initially granted, it is now self-funding through funds obtained from the conferences it runs,[176] although the Audit Office of NSW, NSW Independent Commission Against Corruption, NSW Ombudsman and the NSW Police Service provide some support (http://www.corruptionprevention.net/).

The impetus behind the development of such a network, and its benefits, were outlined to the Committee by Mr Stephen Horne, Performance Audit Director of the NSW Audit Office:

> We also set up what I now believe to be one of the most significant underlying support mechanisms to [assist in fraud prevention], and which I would recommend to anyone, which was the corruption prevention network. A lot of people in agencies said: well, this is great. We've now got a [fraud control] guide, a best practice guide. We can touch it and feel it and it is great. But I'm one person in an agency of 200, 300, 500,000 and my job is fraud control. Who else do I talk to about this? There's no one else here who will talk to me, but there will be someone in the next department and someone in the next department. But there was no mechanism by which they could ever get together.
>
> They were all writing codes of conduct themselves and no one knew what a good one looked like. They were all dealing with reporting problems and all the same problems but re-inventing [solutions]… So we thought, let us bring them together. So we just got a self help group going which started with very humble beginnings. Those that were interested came together… over a cup of coffee at lunchtime, and we soon agreed that we should formalise this and make it a more constructive thing where people could get together and we would exchange information and material…

176 Mr Stephen Horne, Performance Audit Director, NSW Audit Office, in conversation with the Committee, 25 June 2003.

> This has now grown to a network that has run for 10 years, has got its own Web site, holds a large conference each year, has an active email group where you can ask a question: has anyone dealt with frequent flyer points in their fraud policy, and if so, how? And you will get inundated with hundreds of replies. So you don't have to contact everybody.[177]

Following the success of the CPN, a similar organisation has recently been launched in Queensland. The aims of Corruption Prevention Network (Qld) Inc are to:

- facilitate communication between members of the network to help in developing strategies to prevent corruption and improve the ethical conduct of staff;
- provide opportunities for members to access prevention materials and share experiences; and
- assist in effectively implementing best practice in corruption prevention in the Queensland public sector (http://www.cpnq-corruption.net/main.html).

Such networks that give people involved an opportunity to discuss relevant issues are considered essential, because without them there is a risk that fraud control will be just an additional aspect of compliance for people.[178] Unless people are interested and engaged, measures taken are unlikely to be as effective as they could be. There is also likely to be a loss of efficiency as people seek to reinvent the wheel.

Recently the New South Wales CPN has sought to broaden its scope by inviting any interested parties from Australia and overseas to participate. Notwithstanding this move, it remains a predominantly New South Wales-based organisation, with a vast proportion of its members residing in that state. Much of the information on its web site is also New South Wales specific. While it would be possible for interested Victorian parties to join the CPN, the Committee believes it would be preferable to establish a Victorian equivalent, in which the specific fraud control framework and issues that exist in this state could be discussed. The Committee recommends that steps should be taken to facilitate the establishment of such a network, including the provision of seed funding if necessary. The existence of the network should be promoted by VFIRC.

177 Ibid.
178 Ibid.

Recommendation

23. The Committee recommends an informal fraud prevention and control network, such as the New South Wales Corruption Prevention Network, be established in Victoria. Steps should be taken to facilitate the establishment of such a network, including the provision of seed funding if necessary. The existence of the network should be promoted by VFIRC.

Registers

The creation and maintenance of registers containing specific information that can be used for fraud prevention also assists in the fight against fraud. The following sections discuss some of the possible registers that could be developed in this area.

Identity fraud register

The Committee was informed that a serious difficulty exists in responding to the problem of identity-related fraud because public sector agencies and private sector organisations tend not to share information and intelligence about the manner in which such offences occur. Often offenders will employ similar criminal methodologies which, had they been known by other potential victims, would have enabled steps to have been taken to prevent further similar crimes from being perpetrated.[179]

The possibility arises, therefore, that some central agency could compile information on the manner in which identity-related fraud occurs, what fictitious identities are being used, what victims are being targeted and what false documents have been created. Subject to appropriate protection designed to secure the information, this could be shared by agencies with a particular interest in such conduct. Law enforcement agencies would stand to benefit greatly from such intelligence (which is already shared among police services), but appropriate private sector organisations, particularly financial institutions, would also derive a benefit from having access to some or all of these data.

Such a strategy is needed because many different agencies encounter instances of identity fraud but do not share relevant intelligence with each other sufficiently. This impedes a full understanding of the nature and extent of the problem. For example, some individuals have used the same fraudulent identity across a number of different agencies, even after one of those agencies has detected the problem. Had the first incident been publicised, other potential crimes could have been prevented.

The benefits to be derived from such an approach would include the following:

- the ability to identify fraudulent identities that are being used to perpetrate fraud so that further crimes could be prevented;

179 Mr Chris Clark, Acting Director, Australian Crime Commission, in conversation with the Committee, Canberra, 24 June 2003.

- the ability to carry out investigations resulting from an awareness of new fraudulent identities being used;
- a greater appreciation of the use of some fraudulent proof of identity documents;
- a greater understanding of the extent of identity fraud and its impact on organisations;
- the creation of a formal network to exchange identity fraud intelligence; and
- the development of a network to facilitate inquiries with other participating agencies relating to identity fraud investigation.

In addition to the creation of a Register of Identities that have been used unlawfully, the Committee heard suggestions that three additional registers could be created:

- A Victims of Identity Fraud Register;
- A Stolen/Lost Document Register; and
- A Document Image Register.[180]

The proposed Victims of Identity Fraud Register would allow people who have had their identities stolen to notify the register of that theft. This would enable the victim's identity details to be shared with participating agencies, to help reduce the risk of offences being committed in his or her name. Clearly the inclusion of a victim's name on the register should only take place with his or her consent. It would be up to the victim to provide the relevant details to the register, although such notification should be encouraged. The register would also need to be kept secure, with access only being provided to relevant law enforcement or government agencies.

The proposed Stolen/Lost Document Register would operate similarly, but instead of victims notifying the register of their general identity details they would notify the register of the specific details of the evidence of identity documents that have been compromised or lost. The register would display the numbers of all lost documents according to the type of document (eg. passport, birth certificate, etc). Participating agencies would be able to search this facility when provided with such a document, to ensure that it does not belong to someone who has reported it as lost or stolen. The Committee heard that the British Passports Office and the Swedish National Police are independently considering such a scheme, and that INTERPOL has recently announced a similar scheme. The rationale behind such a register is a belief that publicising the type of identity document and the corresponding number to the public greatly diminishes the value of the stolen document.

The proposed Document Image Register would be slightly different. This would be a database of images of evidence of identity documents from around

180 Ibid.

Australia (and New Zealand), with details of security features to aid verification. It is proposed that such a register would have different levels, each of which would only be accessible to those with appropriate security clearance. The first level would show a digital image of the document, and highlight some basic security features. This should be accessible to counter staff of agencies who receive evidence of identity documents on a daily basis, or to fraud managers within organisations. The second level would display more security features, but should only be accessible to law enforcement and specified government agencies. The third level would show all security features, as well as examples of how they have been fraudulently reproduced, and should only be accessible to document examiners employed by law enforcement agencies.

It is anticipated that such a system would assist users to ascertain whether a document is genuine, even if they are not familiar with that particular document. A similar kind of register, on a global scale, has already been created by INTERPOL and is for sale by a commercial publisher.[181] The *Interpol Identity Checker*, is a loose-leaf handbook which provides information on the most important security features of national passports and identity cards for Europe, China, Hong Kong, India, Pakistan, Bangladesh, Nigeria, Jamaica and other countries. Although the *Identity Checker* covers the New Zealand national passport, it does not cover Australian documents. However, an online database covers both the Australian and New Zealand national passports.[182] Explanations are given of the security features used, such as watermarks, UV reaction devices, security threads, Imageperf, lamination techniques, holograms, kinegrams and OVIs. A checklist is also contained for document inspection for use by counter staff, and the handbook is regularly updated.

Recommendations

24a The Committee supports the permanent establishment of various registers concerning identity-related fraud, to be administered either by the Australian Crime Commission or the Australian Federal Police. They would include a register of fraudulent identities and associated fraudulent documents, a victims of identity fraud register, a stolen/lost document register and a document image register.

24b. The Committee recommends that in order to facilitate the establishment of these registers, the Attorney-General for the State of Victoria propose their establishment at the next meeting of the Standing Committee of Attorneys-General.

181 Keesing Reference Systems, *Interpol Identity Checker*, http://www.keesingref.com.

182 http://www.documentchecker.com.

Banned, deregistered or disqualified people registers

In Chapter 6 it was noted that there is a substantial risk of people who have committed fraudulent acts in the past re-offending.[183] Evidence given to the Committee expressed a need to identify publicly those who have committed such acts, in order to prevent them from doing so again.[184] One way to do this could be through the establishment of registers that focus on the perpetrators of fraudulent or dishonest conduct. Such registers could list those who have been convicted of fraud-related offences, as well as those who have been deregistered from professional associations or other organisations for fraud-related conduct. The information contained on such registers would be available for limited disclosure to agencies and organisations seeking to verify the prior history of people in high-risk situations. This would help to prevent, for example, people with prior convictions for dishonesty-related offences failing to disclose these in employment applications or resumes. It would not be appropriate for the register of prior convictions to be made generally available for public inspection. The Committee recommends that VFIRC should have the responsibility for determining in which situations access to the registers should be provided.

One register could be maintained by the Australian Securities and Investments Commission (ASIC). ASIC already maintains a Disqualified Persons Register, which contains a list of people who have been disqualified from involvement in the management of a corporation.[185] The information in the register is readily accessible to the public through information brokers as well as through the Internet (http://www.asic.gov.au/). Unfortunately the register does not contain details of all people who have been disqualified from managing corporations. There are a number of grounds under Part 2D.6 of the *Corporations Act 2001* (Cth) for which a person can be so disqualified. While ASIC is required by the Act to be notified of some such disqualifications, there is no statutory requirement that they be notified of all disqualifications. Only those disqualifications of which ASIC must be expressly notified are included in the register.

So, for example, while section 206B of the *Corporations Act* requires that people convicted of offences that involve dishonesty and are punishable by at least three months' imprisonment be automatically disqualified from managing a corporation for five years,[186] it does not require ASIC to be notified of such

183 See, for example, Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

184 Mr Dennis Challinger, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

185 ASIC also maintains a number of registers in relation to those who have been banned from operating within the financial services industry (http://www.asic.gov.au/asic/ASIC_SRCHLODG.NSF/byid/ CA256AE9000356AECA256AFB008381E5?opendocument).

186 The five-year period begins from the date of conviction if no prison sentence is imposed, or from the date of release if a prison term is served.

disqualifications. As a result, such people may not currently be included in the Disqualified Persons Register.

The Committee believes that ASIC should be notified of all people disqualified from managing a corporation due to a dishonesty-related conviction. It recommends that such information should be included in an appropriate register. By listing the names of such disqualified people on a register, ASIC would provide a valuable source of information to people in the business world about the standing of individuals with whom they conduct business and who may be seeking positions in management (Smith 2002b).

The Committee recommends that a similar system be introduced into Victoria, in relation to business proprietors and proprietors of incorporated associations. People convicted of an offence that involves dishonesty and is punishable by imprisonment for at least three months could be listed on the register and disqualified from being business proprietors or office bearers, members of the committee of management, and public officers of incorporated associations. The Office of Consumer and Business Affairs Victoria should be notified of any such disqualification, for inclusion in any register that it develops and maintains.

The Committee also believes that all Victorian professional regulatory agencies, such as the Legal Practice Board and the Medical Practitioners Board of Victoria, should be required to develop and maintain publicly accessible registers of those who have been deregistered due to fraud or other dishonesty-related offences. This would assist those who seek the services of professionals in a regulated field to ensure that they are fully aware of any history the individual may have of dishonesty-related conduct. At present, while such information may be accessible through the annual reports of such agencies, it is generally not easy to obtain. If such agencies maintained registers, anyone with a legitimate interest in employing someone who is or was a member of the relevant association would be able to seek information concerning any history of dishonesty. The Registrar of the relevant agency would be responsible for determining to whom the information contained on the register should be released.

In order to co-ordinate the provision of such information and to avoid the need for people to approach a variety of different agencies, the Committee also recommends that VFIRC develop and maintain a central service which contains registers of all those who have been deregistered due to fraud or dishonesty-related conduct. Professional associations should be required to notify VFIRC when one of their members has been deregistered for such reasons, for inclusion in VFIRC's central register. Once again, the Committee recommends that VFIRC staff should have the responsibility for ensuring that information from such registers is provided to persons with a legitimate reason for seeking the information.

Recommendations

25a. The Committee recommends that the Australian Securities and Investments Commission be notified of all people disqualified from managing corporations due to dishonesty-related convictions, for inclusion in the Disqualified Persons Register.

25b. The Committee recommends a similar registration system be introduced in Victoria within the Office of Consumer and Business Affairs, in which people can be disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations if they have been convicted of an offence that involves dishonesty and is punishable by imprisonment for at least three months.

25c. The Committee recommends that the Office of Consumer and Business Affairs Victoria be notified of any people who have been disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations due to dishonesty-related convictions, for inclusion in a Victorian Disqualified Persons Register which it develops and maintains.

25d. The Committee recommends that all Victorian professional regulatory agencies, such as the Legal Practice Board and the Medical Practitioners Board of Victoria, be required to notify VFIRC when one of their members has been deregistered due to fraud or dishonesty-related conduct, for inclusion in a register to be maintained by VFIRC. Each professional association should also be required to maintain its own registers of those who have been deregistered due to fraud or other dishonesty-related offences.

25e. The Committee recommends that information on VFIRC's register be made available to persons seeking it for legitimate reasons and that the disclosure of information by VFIRC be carried out in accordance with privacy principles.

Business and Internet domain name registration

One of the key means of carrying out a fraudulent enterprise involves the creation of business or corporate entities and names that can be used as the vehicle for dishonest practices, but which will disguise the true identity of the perpetrator. Misuse of business and corporate names lies at the heart of many types of fraud. For example, stolen cheques can be paid into an account opened in the name of a business that has been registered using a name nearly identical with that of the legitimate cheque payee. Often the slight discrepancy in name will not result in the cheque being returned, or the transaction queried.

In the world of electronic commerce, as described in Chapter 4, a number of recent dishonest practices have relied on the use of misleading or deceptive Internet domain names. Difficulties are encountered by law enforcement

agencies when investigating online fraud if those responsible for registering domain names are unable to be located.

Following a long period of negotiation beginning in 1995, the organisation .au Domain Administration Ltd (auDA)[187] was formed in Australia in 1999 as an industry body to manage Internet domain names. In December 2000 the Australian Government formally endorsed auDA as the appropriate self-regulatory body to administer the .au domain space. As manager of the .au domain, auDA carries out the functions of developing and implementing domain name policies, licensing 2LD registry operators, accrediting and licensing registrars, implementing consumer safeguards, running a centralised information service 'WHOIS',[188] facilitating .au Dispute Resolution Policy, and representing .au at international fora.

AusRegistry is the registry for the five open .au Second Level Domains (2LDs) such as '.com.au' and '.net.au' which are open to all, and others such as '.gov.au' and '.edu.au' which are closed (in that they are limited to government agencies and educational institutions, respectively).[189]

Where individuals or corporations wish to register a domain name they must approach a Registrar, provide limited information concerning the entity to be registered, and pay an annual fee. At present auDA has accredited 19 Registrars, which means that they are authorised to provide Registrar services. Accredited Registrars are also required to comply with the .au Domain Name Suppliers' *Code of Practice*.

The fraud risks associated with such a system are that false and misleading information could be used when registering a domain name, and that names similar to existing domain names could be registered with the intention of misleading consumers. Of greater concern is the possibility that domain names similar to existing government agencies' domain names could be registered, again to deceive consumers into supplying personal information or bank account details online.

The Committee heard of a number of instances in which acts of dishonesty had been committed after individuals registered businesses or created domain names by providing false information to Registrars.[190] In order to solve this problem the Committee believes that more stringent procedures should be in place to verify the information that individuals provide when registering businesses, incorporated associations, incorporating companies, or when applying for domain names. In particular, the process of obtaining a domain name, which at present can take place entirely online, needs to have more extensive verification checks in place. The Committee believes that the

187 http://www.auda.org.au.

188 http://whois.ausregistry.net.au/.

189 http://www.ausregistry.com.au/.

190 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, Sydney, 25 June 2003.

registration of businesses, incorporation of companies and obtaining domain names should be governed by the same verification procedures used when creating an account with a financial institution. The misuse of business entities and domain names is often an essential first step in the commission of large-scale financial crime.

Recommendation

26a. The Committee recommends that the procedures associated with the identification of persons who seek to register a business or incorporated association in Victoria be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of business proprietors or individuals who register an incorporated association.

26b. The Committee recommends that the *Business Names Act 1962* (Vic) be amended to require the Commissioner of Consumer Affairs not to register business names closely similar to existing names and likely to be confused with or mistaken for each other.

27a. The Committee recommends that the Attorney-General for the State of Victoria correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the identification of persons who seek to incorporate a company, to require them to provide the same evidence of identity of the person seeking incorporation as is necessary to open an account with a financial institution. The correspondence should also include a request that procedures be put in place to assist in detecting the use of false information concerning the names of directors and office bearers of companies.

27b. The Committee recommends that the Attorney-General for the State of Victoria also correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the choice of company names, so that company names closely similar to existing names and likely to be confused with or mistaken for each other not be registered.

28a. The Committee recommends that the procedures associated with the identification of persons who seek to register Internet domain names be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of registrants of domain names.

28b. The Committee recommends that the system of registering Internet domain names be reformed to prevent the registration of misleading domain names.

Conclusion

Information lies at the heart of fraud control, both in the pre-digital age as well as in the world of electronic commerce. As discussed, an extensive number of organisations now exist in both the public and private sectors whose aim is to provide information on fraud risk minimisation. What may be needed for the future is for the provision of this abundant information to be better co-ordinated. It is here that the Committee's proposal to create VFIRC would be of great help in enabling consumers to locate the most appropriate source of information quickly and easily from one location, rather than having to visit numerous different organisations.

The other important feature of fraud control discussed in this chapter is the need to have effective systems of registration in place for key activities concerning the registration of businesses, companies and Internet domain names. Most fraudulent activities rely on the use of business entities as a vehicle for the commission of crime or to launder the proceeds of crime. By strengthening and enhancing registration procedures, particularly concerning the identification of registrants (be they individuals or corporate entities themselves), the task of locating those responsible for the commission of economic crime would be facilitated greatly. Some of the Committee's recommendations may lead to registration processes becoming somewhat more complicated, but the benefits to be derived from reduced levels of fraud in the community would greatly outweigh any minor inconveniences and costs involved in strengthening administrative procedures.

8. Detecting and Reporting Fraud

Introduction

The primary barrier to criminal prosecution lies in encouraging those who have suffered loss at the hands of offenders to report their complaint to the authorities. Some, such as those who fall prey to bogus charitable solicitations, may never realise that they have been victimised. They may simply part with funds in the belief that they will be used for the legitimate purpose for which they were intended. Only rarely will a benefactor verify the identity of an individual collecting for a charity, particularly if the organisation is unregistered and does not qualify for tax deductibility status. Thus, as noted in Chapter 3, a number of offences may never be identified as such and reported for criminal investigation. This chapter examines some of the ways in which the detection of fraud can be enhanced. It starts by looking at steps that can be taken within an organisation to detect crimes of dishonesty, including the use of fraud detection software, data matching and the vexed question of those who report fraud in the public interest – so-called 'whistleblowers'. It then focuses on some ways in which fraud can be externally detected, such as through the use of auditors or Internet sweeps. It concludes with an examination of when, how and to whom suspected fraud should be reported. The investigation of suspected fraud is discussed in Chapter 9.

Internal detection

There are a number of ways in which an organisation can internally detect fraud. Some involve the use of computer technologies, while others rely on more traditional methods such as convincing people to come forward and report dishonest behaviour. Some of the more common internal fraud detection measures are discussed below.

Fraud detection software

If it is not possible to prevent fraud entirely, it may at least be possible to identify the presence of fraudulent transactions quickly in order to reduce the extent of any losses suffered or the occurrence of repeat victimisation. One way in which this can be done is through the use of fraud detection software. A

number of organisations have developed such software, which has been specifically designed to assist in detecting a variety of different types of fraud. For example, software has been developed to analyse user spending patterns so as to alert individuals to the presence of unauthorised transactions (see Potter 2002).

The Committee heard that banks often use such software, known as artificial neural networks, to identify anomalous patterns in spending on behalf of their customers.[191] If such patterns are identified, access to the relevant account can be suspended, while the genuine account holder is contacted to ensure the spending is legitimate and authorised. Such software has been seen to be a 'great tool' for detecting fraud, particularly fraud involving credit cards.[192]

The use of computer software to monitor the business activities of government agencies has also been found to provide an effective means of detecting fraud and deterring individuals from acting illegally. The Australian Health Insurance Commission, for example, also employs artificial neural networks to detect inappropriate claims made by health care providers and members of the public in respect of various government-funded health services and benefits. In 1997/98, this technology contributed to the Commission locating $7.6 million in benefits that were paid incorrectly to providers and the public (Health Insurance Commission 1998). In conversations with the Committee, the Director of Fraud Prevention and Control at the Australian Taxation Office (ATO) noted that it also regularly uses networking software to help identify at-risk transactions or taxpayers.[193]

The success of such software, however, depends upon the extent to which it cannot be interfered with or modified. It should not be assumed that fraud will automatically be detected simply by using such software, particularly if the fraud is being perpetrated by those in management positions. In addition, one submission to the Committee noted that software, although regularly used by large financial institutions, is often beyond the means of smaller businesses. This can make these businesses a target for criminal organisations that may be aware of their greater vulnerability.[194]

191 Mr Jilluck Wong, Regional Director, Fraud Prevention, American Express, in conversation with the Committee, 25 June 2003.

192 Submission from Mr Glenn Bowles, bRisk Australia Pty Ltd, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003.

193 Mr Peter Zdjelar, Director of Fraud Prevention and Control, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

194 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

Internet usage monitoring

Another way in which fraud may be detected is by monitoring employees' Internet usage. Employees' use of computers and their online activities can be monitored through software which logs usage and allows managers to know, for example, whether staff are using the Internet for non-work-related activities, or if funds are being transferred for unauthorised purposes. Where certain online activities have been prohibited, many government agencies now monitor the activities of their employees to ensure compliance, sometimes covertly (such as through video surveillance or checking email and files transmitted through servers).

Filtering software may also be used to prevent staff from engaging in certain behaviours. 'Surfwatch', for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user's ID with the content allowable for the assigned category, then either loads the requested page or advises that the request has been denied. The software also logs denied requests for later inspection by management. Although this can be an effective risk management tool for managers, it is possible to bypass filtering software by obtaining the password of the person who installs the software.

While such measures can assist in detecting fraud, it is important to ensure that they are used appropriately. In particular, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers can be used for private activities, if at all. If agencies do permit staff to make use of computers for private purposes then procedures should be in place to protect the privacy and confidentiality of communications, subject to employees obeying the law.

In Australia in March 2000, the Office of the Federal Privacy Commissioner published guidelines on workplace email, web browsing and privacy. These guidelines aim to assist public sector agencies in developing appropriate workplace practices regarding the use of information technologies by employees. They require openness by agencies communicating with staff about what is and what is not permitted in the workplace. They also require agencies to inform staff about the nature and extent to which their computer-related activities are logged and who in the organisation has access to the logged information (Office of the Federal Privacy Commissioner 2000).

More recently, the New South Wales Law Reform Commission (2001) has examined this issue. It has recommended a comprehensive scheme to protect the privacy of employees, including requiring employers to advise employees of their Internet monitoring policy, and to seek a court order if they want to conduct covert surveillance. The Victorian Law Reform Commission (VLRC) is also currently considering this issue in relation to its reference on privacy.[195]

195 http://www.lawreform.vic.gov.au.

Without precluding any specific measures that may be recommended by the VLRC, the Committee believes that, at the very least, employees should be clearly advised of the extent to which they can use computers for their own purposes. In addition, the Committee recommends that prior to employers monitoring their employees' use of the Internet, employees should be informed that they may be monitored. Not only are such measures fair, but they should ensure that employees know the risks they face if they use the Internet inappropriately, as well as precluding them from raising a defence of ignorance if they are caught engaging in unauthorised activities.

Recommendation

29. The Committee recommends that prior to employers monitoring their employees' use of the Internet, employees must be informed that they may be monitored, and be advised of the extent to which they can use computers for their own purposes.

Data matching

In the early 1990s an important strategy was devised to control revenue fraud. The Australian government established an extensive database that sought to reduce taxation and social security fraud by identifying individuals who made claims for benefits from government funds to which they were not entitled.

The Parallel Data-Matching Program, introduced on 23 January 1991 by the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth), allows records relating to specified Tax File Numbers to be compared with payment records held by the main Australian government departments providing benefits, so that anomalies can be identified and targeted for further investigation. It also enables identification of those individuals who are entitled to receive benefits that they have not claimed. In the year 1996/97 the program resulted in 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 $25 million, resulting in a net saving of $132 million (Centrelink 1997).

The ATO Assistant Commissioner told the Committee that the Office engages in a range of data-matching activities in an attempt to detect fraud. For example, it has links with state births, deaths and marriages registries, so that Tax File Numbers can be deactivated upon a person's death to ensure they cannot be used fraudulently. Similarly, it has links with the Department of Immigration, Multiculturalism and Indigenous Affairs (DIMIA), which allow it to be informed when a taxpayer leaves the country. This enables a warning flag to be raised if that individual's Tax File Number is used while they are away. It also has links with a number of other agencies, including Centrelink, the Australian

Transaction Reports and Analysis Centre (AUSTRAC) and state road traffic authorities.[196]

The ATO Assistant Commissioner stated that such matching, as well as data validation (see Chapter 6), can increasingly be performed in real time. For example, when an individual or company applies for an Australian Business Number (ABN), verification about details provided, such as the Tax File Number, address, date of birth and other relevant tax information, is checked while the application is being typed. If problems are identified, the application can be refused. To alleviate privacy concerns, the ATO does not retain such information if it is correct. Such information will only be stored if a problem is identified.

One problem faced by agencies that wish to undertake a data-matching process is that each agency stores its data in very different formats. Each agency will have its own identification number, as well as storing different pieces of information about an individual, depending on what is relevant to that particular agency. This makes it difficult to match data across agencies. At present, attempts to match data rely on using a number of different identifiers that are likely to exist across agencies, such as an individual's name, address, Tax File Number, Centrelink number and Medicare number.

It was suggested to the Committee that this issue could be resolved by introducing a standard format across agencies for the storage of their data.[197] Alternatively, it would be possible to provide each individual with a unique national identification number. While the Committee supports standardising the format in which agencies store their data, it does not support the introduction of unique identification numbers. Identification numbers pose the same risks and problems as identity cards (see Chapter 6). Not only are they potentially privacy-invasive, but they are also easier to compromise than the current system which relies on multiple identifiers. In addition, once they are compromised there can be great difficulty in rectifying the situation.

The Committee notes further that the Parallel Data-Matching Program has not been free from criticism. Most criticism has been directed at the covert way in which data-matching takes place and that Tax File Numbers are now linked to a wide variety of government agencies. There have also been allegations of irregularities and mistakes in matching which have resulted in individuals being wrongly identified as having improperly received government payments (see Birmingham 1995). Due to such concerns, the Committee believes it is important that public sector fraud control initiatives like this program be monitored by an independent body such as the Australian National Audit Office.

196 Mr Greg Dart, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

197 Mr Neil Mann, Deputy Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

Recommendation

30. The Committee recommends that a system of unique identification numbers should not be introduced at a national or state level.

Whistleblowing

The previous sections of this chapter have looked at some of the procedures organisations can have in place to detect fraud. The use of such measures, along with other internal controls such as those discussed in Chapters 5 and 6, is generally seen to be one the most effective ways to detect fraud. For example, in the most recent Ernst & Young survey (2003) internal controls were ranked by respondents as being the best way to detect fraud, while in KPMG's 2002 *Fraud Survey* internal controls were seen to account for 23 per cent of the cases in which fraud was detected.

The other way in which fraud is most commonly detected is through the use of 'whistleblowers'. Whistleblowers are people who reveal wrongdoing within an organisation to the public or to those in positions of authority. They are typically employees of the organisation in question, although any individual who comes into contact with an organisation and discovers such wrongdoing could potentially 'blow the whistle'. In Ernst & Young's *8th Global Survey* (2003), whistleblowing was seen to be the second most effective method of fraud detection, while in KPMG's *Fraud Survey* (2002) 25.7 per cent of fraud was detected by employee notification, with a further 9.1 per cent being notified to the organisation by one of its customers.

The importance of whistleblowing as a method of fraud detection was noted by a number of parties who gave evidence to the Committee. A representative from the New South Wales Audit Office, for example, saw whistleblowing as vital, due to the difficulties in finding fraud in other ways.[198] Representatives of the Corporate Crime Liaison Group (CCLG) and KPMG also commented on the difficulty in detecting fraud through external investigations, noting that in their experience it is most commonly found due to whistleblowing.[199]

It is therefore clear that people with information about white-collar crimes, particularly large-scale fraud, should be encouraged to come forward and report the information to authorities. This would help to ensure that similar patterns of offending by the same or other offenders are uncovered by police and would also reinforce feeling in the community that fraud is unlawful and results in prosecution where it is detected.

198 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

199 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

Unfortunately, there is a significant impediment to the reporting of white-collar crime. This is the fear that some individuals have of reporting matters in the public interest where this may result in their being discriminated against or otherwise subjected to harassment, intimidation or reprisals. This will be a particular problem if the wrongdoing is being committed by those in management. In such circumstances, individuals may reasonably fear that if they speak up, their employment with the organisation may be placed in danger. Addressing this problem was seen to be vital by a number of people who gave evidence to the Committee.[200]

Public sector protection

In an attempt to overcome such an impediment, the Victorian government has enacted the *Whistleblowers Protection Act 2001* (Vic). This Act, which has been in full effect since 1 January 2002, attempts to provide protection for public sector 'whistleblowers' – those who disclose improper conduct or detrimental actions by public officers and public bodies (see Department of Infrastructure, Victoria 2002). Improper conduct includes corrupt conduct, the definition of which would clearly encompass much fraudulent activity relevant to this Inquiry. The Act sets out procedures for both disclosure and investigation, and under s.109 exempts documents connected to protected disclosures from the ambit of the *Freedom of Information Act 1982* (Vic). It amends the *Ombudsman Act 1973* (Vic) and the *Police Regulation Act 1958* (Vic) to similar effect. Offences are created in relation to taking reprisals against a whistleblower (s.18), revealing confidential information related to a protected disclosure (s.22), obstructing an investigation (s.60) and making a false disclosure (s.106).

The aims of this Act were strongly supported in one of the Auditor-General's submissions to the Committee, in which it was noted that:

> Assurance of protection to persons who bring attention to suspected or alleged improper conduct is … a significant catalyst to engendering confidence in the integrity of organisational strategies on fraud prevention. The State's whistleblowers legislation has this underlying aim. Public sector agencies should therefore enthusiastically embrace this legislation and demonstrate to employees and others that they are serious in their desire to act on allegations of improper conduct within their workplace.[201]

The Committee agrees that this Act plays an important role in fraud detection, by offering some protection to those in the public sector who disclose acts of wrongdoing. The Committee believes that its provisions should be publicised

200 Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre (AUSTRAC) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002; Mr Tom Jambrich, Assistant Auditor-General, New South Wales Audit Office, in conversation with the Committee, 25 June 2003; Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

201 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

as widely as possible. This could be one of the roles undertaken by the Victorian Fraud Information and Reporting Centre (VFIRC).

Private sector protection

While the *Whistleblowers Protection Act 2001* (Vic) offers protection to those in the public sector, no such protection is offered to those in the private sector.[202] This means that employees within private sector organisations may face a real risk of reprisals if they speak out against others within their organisation. The Committee believes that those outside the public sector are just as deserving of protection as those in the public sector, and recommends extending the scope of the *Whistleblowers Protection Act 2001* (Vic) to cover them.

Protection for those outside the public sector already exists in some other jurisdictions. For example, under the South Australian *Whistleblowers Protection Act 1993*, anyone who discloses 'public interest information' is protected. While the definition of 'public interest information' covers such public sector wrongs as the maladministration of public officers, the irregular use of public money and the substantial mismanagement of public resources, it also includes wrongs that could equally be perpetrated by the private sector. For example, it covers illegal activity or conduct that causes a substantial risk to health and safety, or to the environment. The Queensland *Whistleblowers Protection Act 1994* also protects public interest disclosures, which include those that relate to a substantial and specific danger either to the health and safety of a person with a disability or to the environment, or if the disclosure is of a reprisal taken against a person who themselves made a public interest disclosure.

The desirability of offering such protection to those outside the public sector was noted in evidence given to the Committee by Mr Newlan, Secretary of the CCLG.[203] It has also recently been discussed by Standards Australia, which released Standard AS 8004-2003 *Whistleblower Protection Programs for Entities* as part of its Corporate Governance package (see Chapter 5). In the Foreword to that Standard, it stated that:

> A whistleblower protection program is an important element in detecting corrupt, illegal or other undesirable conduct… within an entity, and as such, is a necessary ingredient in achieving good corporate governance.
>
> An effective whistleblower program can result in–
>
> (a) more effective compliance with relevant laws;

202 Very limited protection is provided in the specific case of those who provide information or documents to the ACCC or to the Australian Competition Tribunal. Section 162A of the *Trade Practices Act 1974* (Cth) provides for penalties of up to 12 months' imprisonment for individuals and fines of up to $10,000 for corporations who intimidate individuals who report matters (Bhojani 2002).

203 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003. See also Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

(b) more efficient fiscal management of the entity through, for example, the reporting of waste and improper tendering practices;

(c) a healthier and safer work environment through the reporting of unsafe practices;

(d) more effective management;

(e) improved morale within the entity; and

(f) an enhanced perception and the reality that the entity is taking its governance obligations seriously (Standards Australia 2003e, p.4).

Standard AS 8004-2003 sets out a number of elements of a desirable whistleblower protection program. For example, a whistleblower protection policy should be established that articulates 'the benefits and importance to the entity of having such a program as well as the sanctions and disciplinary procedures for non-compliance with the entity's whistleblower protection policy' (Standards Australia 2003e, p.8). There should also be procedures in place for handling any reports received.

Hotlines

An idea that has periodically been advanced to enhance fraud reporting is the use of so-called hotlines. These are telephone numbers dedicated to the reporting of relevant matters. Most commonly, the person receiving the calls will be part of the organisation, such as a manager, although some people may not feel comfortable reporting to someone within their own organisation. It is also possible that the person nominated to receive calls will actually be the perpetrator of the wrongdoing, creating additional difficulties.

To overcome such concerns, some hotlines are externally maintained. Mr Horne of the NSW Audit Office noted that this is an increasingly popular trend in the private sector. Companies will engage a separate organisation to provide a whistleblowing facility. Employees can call the hotline and somebody neutral to the company will take the call. Information can be provided anonymously if desired. Relevant information will then be passed on to the company for investigation.[204]

The Committee believes that externally maintained hotlines are of great assistance in detecting fraud. If people are to be encouraged to report fraud, it is important that they feel comfortable in speaking out. In many organisations, particularly small organisations, this will not be possible if the person to whom wrongdoing must be reported is known to the whistleblower. Potential whistleblowers may feel frightened of that person, or of their possible reaction to their claims. Alternatively, they may not believe that the contact person will properly pursue their allegations. In addition, internal reporting mechanisms

204 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

will rarely provide for the possibility of truly anonymous reporting, even in larger organisations, as there is always a risk that an individual's voice will be recognised. Many individuals may feel more willing to be open and honest if their anonymity is protected.

The Committee recommends therefore that VFIRC establish a hotline for the reporting of public or private sector fraud. It should be possible for people to report anonymously if desired. VFIRC should determine whether further investigation is required, and if so which is the most appropriate body to carry out that investigation. When providing the appropriate body with the information necessary to conduct such an investigation, care must be taken to protect the whistleblower, in accordance with the procedures set out in the *Whistleblowers Protection Act 2001* (Vic). The existence of such a facility should be widely promoted by VFIRC.

Compensation

As discussed above, whistleblowing is an important tool in the detection and reporting of fraud, and the *Whistleblowers Protection Act 2001* (Vic) has been established to encourage whistleblowers to come forward. The Committee has recommended expanding the scope of the Act to cover the private sector, as well as developing an externally maintained hotline to facilitate the reporting of fraud and other misconduct. Such measures will be of little value, however, if people are still reticent to come forward with any information they may have.

As seen above, such reticence may be due to a fear of reprisals. While legal protection is offered by the *Whistleblowers Protection Act 2001*, the Committee believes that the protections offered may still not be adequate.

It is hoped that this issue will be resolved over time as the provisions of the *Whistleblowers Protection Act 2001* are enforced. This legislation is relatively new, and no high profile breaches have yet come before the courts. If breaches are detected, it is hoped that they will be prosecuted fully, showing the community that such behaviour will not be tolerated.[205]

Even if such legislation offers effective protection, however, people may be disinclined to report wrongdoings due to financial or other consequences that may result from taking such action. These can range from the inconvenience of assisting in an investigation or appearing as a witness in court, to suffering extreme financial hardship due to loss of employment.

The Committee believes it would be useful to examine further ways in which these barriers can be overcome. It may, for example, be desirable to establish a fund to provide compensation for financial loss suffered as a result of reporting. This could be achieved by setting aside part of the funds obtained through

205 Mr Tom Jambrich, Assistant Auditor-General, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

criminal confiscation legislation, if the Commonwealth were agreeable to taking these out of consolidated revenue.

It would also be possible to reform current procedures in order to reduce the time and personal costs associated with the investigation and prosecution of matters. For example, interviewing procedures could be streamlined and the need for senior witnesses to be present in court for lengthy periods could be reduced. Documentary evidence could also be used in preference to oral testimony wherever possible. Appropriate use of awards of costs to assist witnesses could also be considered, and scales of witness expenses could be increased to more realistic levels.

Alternatively, it would be possible to provide a financial incentive for whistleblowing by introducing a *qui tam* law similar to that which exists in the United States.[206] This is a provision of the *Federal Civil False Claims Act*, which enables private citizens who have independent and direct knowledge of fraud by government contractors, or other entities who receive or use government funds, to prosecute those contractors in the name of the US government. If successful, such individuals are rewarded with a share in any funds that are recovered, up to a maximum of 30 per cent. The Department of Justice in the United States may join the action with the party who raises the action, or it may decline to do so. If it joins, it will take over the primary role in the case, although the private party retains the right to continue as a party to the action (http://www.quitam.com).

Since the establishment of the *qui tam* law in its current formulation in 1986, recoveries have exceeded US$1 billion, with individual recoveries in cases of this nature being as high as US$150 million. Most successful cases have involved fraud in the defence and health care sectors in the United States. Most commonly the fraud involves the presentation of false claims to the government for payment or approval. This is called 'mischarging', and covers claims for goods or services not actually rendered. An example might be a government employee who charges for time not worked.[207]

Such a law is undoubtedly advantageous to whistleblowers, as they are offered a clear incentive for reporting fraud. It could also be advantageous to the government, which may recoup lost money if claims are successful. In addition, such a law may assist in changing public attitudes towards whistleblowing, so that instead of fearing reprisals 'there is praise, recognition of a service to the public and financial reward'.[208] Conversely, however, it could lead to an increase in vexatious or frivolous claims.

206 Submission from Ms Patricia Farnell, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 August 2003. *Qui tam* is an abbreviation from the Latin *qui tam pro domino rege quam pro sic ipso in hoc parte sequitur*, meaning 'who as well for the king as for himself sues in this matter'.

207 http://www.quitam.com.

208 Submission from Ms Patricia Farnell, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 August 2003.

The Committee does not believe that it is in a position to make recommendations about exactly which of these measures, if any, should be implemented. Many of the measures outlined above extend beyond the scope of the current inquiry. In addition, some of them are potentially far-reaching, and could have significant and unanticipated consequences. For this reason, the Committee believes that the question of whether and how individuals should be compensated for reporting instances of suspected fraud should be referred to the Victorian Law Reform Commission for further inquiry.

Recommendations

31. The Committee recommends that the *Whistleblowers Protection Act 2001* (Vic) be extended to individuals who report suspected fraud and offences involving dishonesty committed in the private sector.

32. The Committee recommends that VFIRC establish a hotline for reporting public or private sector fraud. It should be possible for people to report anonymously if desired. VFIRC should determine whether further investigation is required, and if so which is the most appropriate body to carry out that investigation. When providing the appropriate body with the information necessary to conduct such an investigation, care must be taken to protect the whistleblower, in accordance with the procedures set out in the *Whistleblowers Protection Act 2001* (Vic).

33. The Committee recommends that the question of whether and how individuals should be compensated for reporting instances of suspected fraud should be referred to the Victorian Law Reform Commission for further inquiry. Issues to be addressed by the inquiry should include whether a fund should be established to compensate individuals who have suffered loss as a result of reporting fraud, the desirability of introducing *qui tam* laws in relation to whistleblowers, and whether scales of costs applicable to witnesses in fraud cases should be reviewed.

External detection

Previous sections of this Report have discussed ways in which fraudulent or dishonest conduct can be detected internally. It is also possible, though less likely, that fraud could be detected by external parties. This could occur either with the co-operation of the organisation (for example, by hiring an external auditor) or as a result of the ordinary activities of an external agency working in the area. The following sections examine some of the means by which fraud can be discovered externally.

Auditing

One way in which fraud could be detected is by conducting an audit. While many audits are conducted internally, it is also possible to have them conducted by an external party.[209] In the Victorian Public Service, as well as in various statutorily regulated professions, external audits are required annually. This external monitoring of financial matters in the public sector is performed by the Office of the Auditor-General, which also assists in the development of financial management systems to ensure that expenditure is properly accountable and to encourage timely and accurate reporting of fraud.[210]

There is a common perception that such audits are one of the best ways in which to detect fraud. In reality, however, audits are seen to be 'spectacularly unsuccessful' at discovering fraudulent conduct.[211] This is because auditors cannot individually examine every transaction that has taken place within an organisation. This would be too time-consuming and expensive. Unless there is a suspicion of wrongdoing, auditors tend to focus on higher level transactions and the financial framework as a whole, rather than the smaller transactions that are usually the basis of fraud.[212] This is not to say that an audit can never discover fraud. Auditors may detect fraud occasionally, but it is likely to be a 'fluke'.[213]

This can be seen in the results of recent fraud surveys. KPMG's *Fraud Survey* (2002) found 'external auditor review' to be the least likely way in which fraud was detected, accounting for only 1.1 per cent of cases. An additional 8.6 per cent of fraud was detected by 'internal auditor review'. Similar results were found in Ernst & Young's *8th Global Survey* (2003). Respondents ranked 'external audit' as being the least likely measure to result in fraud detection of

209 Auditing should therefore technically be considered to be both an internal and external means of detecting fraud.

210 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002. For more information on the role of the Auditor-General, see Chapter 5.

211 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

212 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

213 Mr Stephen Horne, Performance Audit Director, New South Wales Audit Office, in conversation with the Committee, 25 June 2003.

the six measures provided: 'most felt that fraud was more likely to be detected by accident than by external auditors' (Ernst & Young 2003, p.6). 'Internal audit' was ranked third, behind internal controls and whistleblowers.

This disjunction between the perception of what auditors can achieve and what they actually can achieve is known as the 'expectation gap'. The Auditor-General of Victoria commented on this gap in a submission to the Committee:

> The general public believes that the auditor should be responsible for detecting all fraud, while the auditing profession believes its responsibilities are limited to planning the audit so that there is a reasonable expectation of detecting material fraud.[214]

Detecting fraud is not actually one of the objectives of an audit, nor is investigating fraud that is discovered. The auditing process is designed to ensure that adequate processes and procedures are in place so that fraud can be identified if it takes place. The precise role of auditors was expanded on in evidence given to the Committee:

> Essentially the accounting profession has said that it is not the responsibility of the auditor to investigate fraud; nor is it the responsibility of the auditor to identify fraud, and that their role is to test the internal control environment within an organisation to establish whether the practices and procedures within that organisation are sufficiently robust to identify when, and if, a fraud occurs. As auditors we need to understand that those systems are robust. At a point where a fraud is in fact identified by an auditor, the general practice has been that fraud is not investigated by the auditor but passed to people who have the skill sets necessary to undertake that investigation themselves.[215]

Therefore it is perhaps better to consider audits as a preventive measure, rather than as a method of detection. The auditing process is valuable insofar as it can help to ensure a sound financial management framework, which is essential to fraud prevention (see Chapters 5 and 6). In addition, the risk that the auditing process may uncover fraud, no matter how unlikely, could also discourage people from committing such acts. The preventative role of auditing was noted in Ernst & Young's *8th Global Survey* (2003), in which internal and external audits were respectively ranked as the third and fourth best ways in which to prevent fraud.

AUSTRAC

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence unit and anti-money-laundering regulator, and is an important source of information and expertise for the detection and

214 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002.

215 Mr Edward Hay, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

investigation of financial crime. In its regulatory role it oversees compliance with the reporting requirements of the *Financial Transaction Reports Act 1988* (Cth) (FTR Act) by a wide range of financial services providers, the gambling industry and others. In its intelligence role it provides financial transaction reports information to Commonwealth, state and territory law enforcement and revenue agencies. AUSTRAC collects, retains, compiles, analyses and disseminates information collected. It also issues guidelines and circulars to those entities required to report cash transactions (called 'cash dealers') about their obligations under the FTR Act and Financial Transactions Reports Regulations 1990 (See Australian Transaction Reports and Analysis Centre 2002).

AUSTRAC's mission is to contribute towards a financial environment hostile to money laundering, major crime and tax evasion. This is done by working to ensure that financial service providers and cash dealers identify their customers and so reduce the occurrence of false-name bank accounts and the like. Through its compilation and analysis functions, AUSTRAC monitors and identifies money laundering related to serious crime and major tax evasion. This financial intelligence is provided to the ATO and Commonwealth, state and territory law enforcement, security and revenue agencies.

AUSTRAC provides the ATO and specified law enforcement, security and revenue agencies with both general and specific access to the FTR information it collects. The general access, governed by memoranda of understanding, is by way of controlled online access to the data and, where appropriate, by extracts of parts of the data holdings. This allows partner agencies to add AUSTRAC's financial intelligence on particular matters to their intelligence pictures, so giving them a better understanding of the activities being examined. The specific access includes referrals of information initiated by AUSTRAC or by the cash dealers that suggest new instances of money laundering.

Revenue authorities in particular are able to make use of the information derived from financial transaction reporting requirements to identify suspicious patterns of cash transactions which could involve illegality or money laundering. In Australia in 1997/98 the ATO attributed more than $47 million in revenue assessed to its direct use of information provided by AUSTRAC. In one case a taxpayer and associated entities had transferred more than $1.3 million to a tax haven. Following an investigation, more than $6 million in undeclared income was detected (AUSTRAC 1999).

AUSTRAC also watches for money-laundering techniques that seek to avoid the formal reporting and identification requirements of the FTR Act. AUSTRAC aims to ensure that the integrity of the system is maintained and that advice is given to the government when further preventive steps may be warranted. AUSTRAC has powers to take court action for injunctive remedies to secure compliance with the requirements of the FTR Act. Criminal sanctions also apply for non-compliance.

While AUSTRAC can offer great assistance to some agencies in detecting fraud, it has been suggested that the full potential of AUSTRAC's financial intelligence has not been realised in responding to fraud.[216] It is to be hoped that in the future this valuable resource is used to its full extent.

Internet sweeps

Another way in which Internet-related fraudulent or dishonest conduct can be discovered is through what are known as 'Internet sweeps'. These are sweeps of the Internet which are conducted in order to identify illegal practices and sites that contain misleading and deceptive information. Such sweeps are regularly conducted by consumer protection agencies around the world.

One of the main proponents of such sweeps is the International Consumer Protection and Enforcement Network (ICPEN), formerly known as the International Marketing Supervision Network (http://www.icpen.org). This is an organisation consisting of the trade practices law enforcement authorities of more than two dozen countries, most of which are members of the Organisation for Economic Cooperation and Development. Since 1997 the ICPEN has conducted International Internet Sweep Days. These have been led by the Australian Competition and Consumer Commission (ACCC) and have incorporated the efforts of Victorian and other Australian agencies.[217] They target dishonest online operations, responding to 'the growing number of fraudulent and deceptive scams emerging on the Internet' (http://www.icpen.org/imsn/activities.htm). The sweeps have so far revolved around themes such as 'get-rich-quick' schemes (1997), bogus medical products (1998, 2002) and compliance with consumer protection principles (1999, 2001) (Australian Competition and Consumer Commission 2001).

The first sweep (aimed at get-rich-quick schemes) in 1997 located over 1,100 suspicious sites, which were sent advisory emails concerning their obligations under consumer protection laws. Two weeks later, approximately 25 per cent of those sites had been removed or altered (Australian Competition and Consumer Commission 1997). A similar sweep co-ordinated by the Federal Trade Commission in the United States, entitled 'GetRichQuick.Con', was conducted in 2000 (Brown & Johnston 2000).

In January 2002, 58 agencies from 19 countries were involved in the sweep. As the Sweep Report states, these co-operative efforts have proved to be 'a cost-effective compliance and public relations tool' (Australian Competition and Consumer Commission 2002b, p.5). However, the sweeps are also beginning to yield concrete outcomes. The ACCC reported in September 2002 that as a

216 Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre (AUSTRAC) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

217 In October 2003 the ACCC stepped down from its 12-month presidency of ICPEN: Submission from Mr Robert Antich, Australian Competition & Consumer Commission, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 3 October 2003.

result of the January sweep, 18 companies were facing legal action and more than 200 investigations were still underway in the participating countries. Out of court settlements had already been reached with Victorian enterprises that were engaged in various questionable businesses. One enterprise had been promoting the use of magnetic fields and colloidal silver suspended in water to cure AIDS and boost the immune system, and another offered to test, diagnose and reverse the ageing process. A third web site was marketing a multi-coloured shirt claimed to relieve stress, make the wearer more intelligent and perceptive, improve concentration, allow continuous exercise and boost the immune system (Australian Competition and Consumer Commission 2002a).

As a result of ACCC action, these improbable enterprises, and others like them, have altered or withdrawn their web sites. The sense in these (still early) days of electronic commerce that 'anything is possible online', and the audacity of offenders quickly seizing those opportunities, appear to be reined in very quickly once the threat of legal action is in the air. This is an encouraging sign, but those waging the war against online scams and marketing ploys are likely to encounter tougher battles in jurisdictions in which consumer protection is not such a high priority.

Reporting fraud

Once an individual or organisation has detected a suspected fraud, a number of questions arise as to what steps should next be taken: Should the activity be investigated further prior to being reported? In what circumstances should it be reported? To whom should it be reported? The answers to these questions will vary, depending on who has discovered the fraud and the nature and extent of the fraudulent activity.

For example, all Victorian public service entities (apart from local government) are required to report all cases of suspected fraud to the Auditor-General and the Minister for Finance. Procedure (c) under Direction 4.3 of the Standing Directions of the Minister for Finance (see Chapter 5) states that the Auditor-General and the Minister for Finance must be notified of 'all cases of suspected or actual theft, arson, irregularity or fraud in connection with the receipt or disposal of money, stores or other property of any kind whatsoever under the control of a Public Sector Agency' (Department of Treasury and Finance 2003b).

In the private sector there are certain circumstances in which an obligation arises to report fraud. For example, there is an obligation on financial dealers to report fraud committed by licensees to the Australian Securities and Investments Commission (ASIC).[218] In general, however, there is no such requirement. This leaves individuals and organisations with a choice about which frauds to report, which to investigate, and which not to pursue any

218 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

further. Many organisations may have a policy in place to help them make this determination, which could refer to factors such as the dollar value of the fraud, or the likelihood of a successful prosecution. For example, in conversations with the Committee an Assistant Commissioner of the ATO stated that they refer all matters considered suitable for prosecution to the Director of Public Prosecutions, who makes a decision about whether to pursue the matter further.[219]

One consequence of this system is that a lot of fraud remains unreported (see Chapter 3). The latest KPMG fraud survey found that nearly four out of every 10 fraud offences were not reported to the police by the victim organisation (KPMG 2002). As noted in Chapter 3, there are a lot of reasons why the reporting rate is so low. These include a belief by individuals or organisations that particular matters are not serious enough to warrant police attention, a fear of losing business or damaging their reputation, a belief that there is inadequate evidence to justify reporting to police, and a reluctance to devote time and resources to prosecuting matters.

There are two main consequences of this low rate of reporting. First, it makes it impossible to understand the precise nature and extent of fraudulent activities being committed in Victoria and Australia. This makes it difficult to know exactly how this problem can best be addressed. Secondly, it can lead to perpetrators avoiding prosecution for their acts. This not only leaves them free to commit such activities against other individuals or organisations but also undermines the development of a culture of intolerance to fraud, which is necessary if the problem is ever to be effectively tackled.

Proposed reporting reforms

One way in which the reporting of fraud could be enhanced would be to require local governments to report fraud to the Auditor-General and the Minister for Finance. As noted above, Direction 4.3(c) of the Standing Directions of the Minister for Finance requires such reporting for all other public sector entities. There seems little reason why the scope of this Direction should not be expanded to also include local government agencies. Such an amendment was suggested by those within the Office of the Auditor-General.[220] It was noted that unless local government agencies are required to report fraud, it is not possible to gain a comprehensive understanding of fraud in the Victorian public sector. Such a requirement was also seen to be particularly important in light of the multitude of activities that take place within the

219 Mr Rory Mulligan, Assistant Commissioner, Australian Taxation Office, in conversation with the Committee, 24 June 2003.

220 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 14 August 2002; Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003; Mr Joe Manders, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

responsibility of municipal councils.[221] The Committee supports such a reform, including providing additional resources to the Auditor-General (if necessary) to enable the investigation of cases notified.

Such a reform, however, would only marginally increase the rate at which fraud is reported. A more significant increase in reporting could be achieved by requiring all instances of fraud to be reported across the board. Such mandatory reporting of fraud was supported by a number of people who gave evidence before the Committee. Those involved in law enforcement, in particular, supported such a reform, as it would permit them to gain a better understanding of what is taking place, which would be useful for intelligence purposes. It would also enable them to make a decision as to which cases it is in the public interest to pursue.[222] This was considered to be preferable to the current situation, in which such decisions are often made by private sector organisations for commercial reasons.

Practitioners and consultants working in the field also supported a requirement that fraud be reported by all organisations. Mr Andrew Tuohy from KPMG, for example, argued that such a requirement would help reach a better understanding of the extent of fraud, although he noted that such an understanding would still not be complete, as there would be some failure to comply with such a requirement. He further stated that such a reform 'would probably promote companies taking matters further', which is recommended by KPMG as best practice in most cases.[223] Similarly, Mr Dean Newlan of the CCLG told the Committee that clients are advised to report matters, and it was his personal view that such reporting should be compulsory.[224] Mr Dennis Challinger saw such a reform as being useful, because it may help to prevent people who have committed fraud from re-offending.[225]

There were, however, concerns expressed about introducing such a system. Mr Andrew Tuohy, for example, argued that any such requirement would have to be 'structured correctly', with the definition of what instances were required to

221 Mr Joe Manders, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

222 Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003; Mr Des Berwick, Executive Officer, Australasian Centre for Policing Research, in conversation with the Committee, 3 October 2003; Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003; Mr Paul Coghlan QC, Director of Public Prosecutions, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

223 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

224 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

225 Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

be reported being clarified sufficiently for 'companies to understand what their obligations are'.[226] Superintendent Philip Masters, Divisional Head of the Major Fraud Investigation Division of Victoria Police, was concerned about the possible increase in workload, noting that it may not be possible to investigate all reports.[227] Additional concerns were raised about the enforceability of such a requirement.[228]

The Committee agrees that careful consideration needs to be given to any such proposal, to ensure that it is clear and backed by additional resources and appropriate sanctions. Such concerns should not, however, be allowed to overshadow the merits of a system of compulsory reporting. As long as due attention is given to these concerns when drafting relevant legislation, the Committee believes they can be adequately addressed.

The Committee believes that a compulsory reporting system would be advantageous for all of the reasons outlined above. Rather than reporting such fraud directly to Victoria Police, however, the Committee recommends that VFIRC be the central Victorian agency to receive all reports of fraud from individuals, public sector agencies and private sector organisations. This would help to ensure that Victoria Police is not inundated with an unmediated deluge of minor matters. It would also assist VFIRC in the collection of fraud-related statistics (see Chapter 3).

All public sector agencies and private sector organisations that become aware of incidents of fraud should be required to notify VFIRC of such incidents within 10 working days. They should also be required to notify VFIRC of the outcome of any fraud-related investigations and prosecutions within 10 working days of the outcome being known or a decision being made. This would allow VFIRC to track the progress of cases, which would provide valuable assistance in evaluating the current Victorian fraud control framework. The Committee recommends that failure to comply with these requirements should be subject to appropriate sanctions.

Proposed reforms concerning serious fraud

The Committee believes, however, that instances of serious fraud should be handled differently and that a criminal offence should be created where there is a failure to report a serious offence involving dishonesty (being an offence within the Australian Standard Offence Classification category of dishonesty). A 'serious offence' should be defined as one in which the victim believes that

226 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

227 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

228 Ms Alison Creighton, Legal Project Officer, Legal and Corporate Policy, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

any financial loss suffered would amount to at least $100,000. A similar offence already exists in New South Wales. Subsection 1 of s.316 *Crimes Act 1900* (NSW) creates an offence of failing to report a 'serious offence' (being an offence punishable by at least five years' imprisonment) to the police where the person knows or believes that the offence has been committed and that he or she has information which might be of material assistance to the police. This offence carries a maximum penalty of two years' imprisonment, though a prosecution of professionals such as accountants who fail to report serious offences cannot take place without the approval of the Attorney-General.

Role of VFIRC

The role of VFIRC should be to act as a clearinghouse. That is, VFIRC analysts would receive reports, compile statistical information and then transmit reports to relevant agencies for investigation. For example (as noted in Chapter 3), a complaint involving misleading and deceptive practices concerning the share market on the Internet could be referred to the Victoria Police Major Fraud Investigation Division, the Australian High Tech Crime Centre, the Department of Business and Consumer Affairs Victoria, the Australian Securities and Investments Commission and other agencies at a federal and state level. VFIRC would not play any role in the investigation of such matters, and should have no investigatory powers.

To assist VFIRC in identifying the appropriate agency to which matters should be referred, it would be necessary for officers at VFIRC to regularly liaise with all relevant agencies. This would include professional regulatory bodies such as the Legal Practice Board and the Medical Practitioners Board of Victoria, Commonwealth agencies such as the Australian Crime Commission and the Australian High Tech Crime Centre, and state agencies such as the Office of the Auditor-General and Victoria Police. It would also be useful for VFIRC to devise guidelines for determining which agency is best placed to investigate reports that have been received. The Committee recommends that VFIRC organise a forum with representatives from all appropriate agencies to help with this task.

The Committee further recommends that VFIRC produce a best practice guide to reporting fraud, including a description of what information should be provided. The guide should contain specific information on preparing reports where the matter is likely to require further police action to be taken. The need for such a guide was noted by Mr Newlan of the CCLG, which currently assists complainants in the preparation of appropriately structured briefing papers for the police.[229] At a broader level, it would also be useful if VFIRC provided guidance to organisations to 'facilitate sound strategic responses to fraud'.[230]

229 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

230 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

While VFIRC would play an important role in determining which agencies reports should be forwarded to, the Committee recommends that all reports received by VFIRC be forwarded to Victoria Police. Attached to such reports should be a statement of which other agencies, if any, the report has been forwarded to, and any recommendations as to whether Victoria Police should act in partnership with such agencies, or with any other relevant public or private sector body (including the victim) in the investigation of the matter (see Chapter 9). VFIRC should also be able to recommend which branch of Victoria Police (such as the Major Fraud Investigation Division or a Criminal Investigation Unit) would be most appropriate to handle the matter. Victoria Police should, however, retain final discretion in deciding how to proceed with any matter.

In conversations with the Committee, Commissioner Hyde expressed a view that despite being required to make such reports, some organisations may be unwilling to do so for commercial reasons.[231] Mr Dennis Challinger similarly noted that smaller organisations may seek to avoid such a requirement, as they may be reticent to get involved in the criminal justice system due to the costs involved.[232] A similar point was made by Mr Edward Hay, the Victorian Deputy Auditor-General, who was 'not persuaded' that mandatory reporting would work, because people will still be making decisions about whether to report based on commercial or other reasons, even if there is such a requirement.[233]

It was suggested that one way in which such reticence could be overcome would be to develop a procedure which would not require all reported cases to be investigated by the police.[234] If people knew that the matter they reported would not, as a matter of course, result in a prosecution they might be more willing to comply with the requirement to do so. While the reporting of cases which are not investigated would obviously not assist in preventing particular offenders from re-offending, the mere fact that a report has been lodged would help in gaining a more complete understanding of the extent and nature of fraud, and in developing strategies and tactics to deal with particular problems. To this end, the Committee recommends that, at the request of a victim, VFIRC be able to recommend to Victoria Police that no further action be taken at all in a particular matter. While it is hoped that such a recommendation would be taken into account, the final decision about investigation should continue to reside with Victoria Police.

Prior to implementing such reforms, it is important to ensure that there are protections in place so that reprisals cannot be taken against those who report

231 Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

232 Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

233 Mr Edward Hay, Victorian Auditor-General's Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

234 Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

matters. As noted above, such protections currently exist in relation to the public sector. It would be necessary to implement the reforms recommended in relation to private sector whistleblowing (Recommendation 31) before requiring people in the private sector to report suspected fraud. In addition, sanctions should be put in place for those who report for other than bona fide reasons.

Recommendations

34a. The Committee recommends that VFIRC be the central Victorian agency to receive all reports of fraud from individuals, public sector agencies and private sector organisations.

34b. The Committee recommends that all public sector agencies and private sector organisations that become aware of incidents of fraud be required to notify VFIRC within 10 working days. The Committee recommends that failure to comply with this requirement be subject to appropriate sanctions.

34c. The Committee recommends that all public sector agencies and private sector organisations be required to notify VFIRC of the outcome of any fraud-related investigations and prosecutions within 10 working days of the outcome being known or a decision being made.

34d. The Committee recommends that a criminal offence be created of failure to report a serious offence involving dishonesty (being an offence within the Australian Standard Offence Classification category of dishonesty) where the victim believes that any financial loss suffered would amount to at least $100,000.

34e. The Committee recommends that VFIRC act as a clearinghouse, determining which is the appropriate agency (if any) to act upon the report, and providing that agency with the report. Relevant agencies would include professional regulatory bodies such as the Legal Practice Board or the Medical Practitioners Board of Victoria, Commonwealth agencies such as the Australian Crime Commission or the Australian High Tech Crime Centre, and state agencies such as the Office of the Auditor-General or Victoria Police. VFIRC should not have any investigatory powers.

34f. The Committee recommends that all reports received by VFIRC be forwarded to Victoria Police. VFIRC should have the power to recommend which branch of Victoria Police (such as the Major Fraud Investigation Division or a Criminal Investigation Unit) would be most appropriate to handle the matter and to recommend that Victoria Police act in partnership with another public or private sector body, including the victim. Where the victim makes such a request, VFIRC should also be able to recommend that no police action be taken at all. Victoria Police would, however, retain final discretion in deciding how to proceed with any matter.

34g. The Committee recommends that VFIRC organise a forum with representatives from all appropriate agencies, to help devise guidelines for determining which agency is best placed to investigate reports that have been received.

34h. The Committee recommends that VFIRC produce a best practice guide to reporting fraud, including a description of what information should be provided. The guide should contain specific information on preparing reports where the matter is likely to require further police action to be taken. Similar information should be published on the VFIRC web site.

35. The Committee recommends that the requirement under Direction 4.3 of the Standing Directions of the Minister for Finance, requiring cases of suspected or actual theft, irregularity or fraud under the control of their departments to be notified to the relevant Minister and the Auditor-General, be extended to all public sector agencies in Victoria including local government departments. The Auditor-General's resources should be increased to deal with any increased caseload.

Conclusion

Ideally, the fraud prevention measures outlined in the previous chapters would eliminate all incidents of fraud. While this is a goal to be strived for, in the meantime it is necessary to ensure that there are measures in place to detect those incidents which continue to occur. The first part of this chapter examined a number of measures that organisations could take to help detect fraud, as well as some ways in which fraudulent conduct could be externally detected. It focused, in particular, on the need to encourage people to come forward and 'blow the whistle' on the perpetrators. This would only be achievable, however, if adequate protections were offered to those who are brave enough to speak out.

The second part of the chapter looked at what should be done once fraud has been detected. At present, there is no requirement to report such fraud outside the public sector. This has led to a very high level of under-reporting, which has the dual consequences of preventing a proper understanding of the nature and extent of such activities being developed, as well as enabling those who commit such acts to re-offend. The Committee has recommended that those who discover fraud be required to report it. It is hoped that this measure will not only lead to a better comprehension of the intricacies of fraud but will also encourage the development of a culture in which fraud is not tolerated.

9. Investigating Fraud

Introduction

In addition to the reluctance of individuals to report white-collar crime, there are many problems associated with the effective investigation of cases. White-collar crime involves the use of highly sophisticated techniques of deception and planning, and offenders often go to considerable lengths to disguise their identity and to make documentary financial trails of evidence difficult to follow. Chapter 8 of this Report focused on ways in which suspected fraudulent conduct can be detected. This leads to the question of how to deal with such conduct once it has been discovered.

White-collar crime has traditionally been dealt with through the legal processes of investigation, employing publicly funded police services; prosecution by state-administered prosecution agencies; trial in the criminal courts, often employing juries; and punishment in the state-administered correctional system. In recent times, many of the state functions noted above have been taken over by privately funded agencies, usually working in conjunction with their publicly funded counterparts. Financial considerations have 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 white-collar crime has, therefore, been severely restricted for financial reasons, though the possibility of criminal prosecution and sanction has always remained open.

One submission received by the Committee noted that the criminal justice system, of itself, will have a diminishing impact on the problem of fraud and that:

> There is a sense of resignation prevailing in the corporate community as to the criminal justice system's apparent inability to suppress the incidence of fraud and to deal with reported fraud in a timely and efficient manner.[235]

235 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

According to this submission,

> The criminal justice system's inability to deal effectively with the commercial crime issue is due to a number of factors including lack of resources generally, outdated and cumbersome legislation, lack of coordination across Australia at the legislative, executive and judiciary levels and an inability to keep pace with technological change.[236]

This chapter examines ways in which the investigative process can be improved, in order to address some of the concerns outlined above and to enhance the response to detected fraud. Chapter 10 then focuses on the rest of the criminal justice process, examining applicable laws and the processes of prosecution and sentencing.

A national response

One of the most difficult problems for those charged with investigating fraud and white-collar crime is the fact that many offences take place across jurisdictional borders, involving offenders and their victims located in different states and territories or even countries. Such multi-jurisdictional crimes are becoming increasingly common, partly as a result of the increase in recent years of organised criminals in fraudulent activity (see Chapter 2). This makes it necessary to develop a national approach to the investigation of such crimes. This was noted in evidence given to the Committee by Superintendent Masters of the Major Fraud Investigation Division of Victoria Police. He saw a national, unified approach to the co-ordination and investigation of electronic crime and fraud-related matters to be essential.[237]

The first steps towards developing a national approach in the area of electronic crime have recently been taken with the establishment of the Australian High Tech Crime Centre (AHTCC). As noted in Chapter 1, the AHTCC commenced operation early in January 2003 and provides a national response to electronic crime, with resources drawn from each state and territory police service. It has all state and territory Police Commissioners on its board of management, ensuring that the focus it takes is one of national priorities, as opposed to a state or federal approach.[238] The merits of the AHTCC were argued in evidence given to the Committee,[239] and the Committee encourages its ongoing development and use in investigating crimes that often know no borders.

236 Ibid.

237 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

238 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

239 Mr Des Berwick, Executive Officer, Australasian Centre for Policing Research, in conversation with the Committee, 3 October 2003.

To assist in the development of a national framework, the Australian Institute of Professional Investigators (formerly the Corporate Crime Liaison Group) and the Major Fraud Investigation Division of Victoria Police are currently drafting policy standards for fraud investigations both in Victoria and across Australia. This initiative was discussed in a submission provided to the Committee, in which it was noted that:

> The working group has established a draft set of policy standards, which encompass the civil and criminal fraud investigation standards. These standards also take into account the Federal Government's certificate level 4 standards for private fraud investigations on behalf of the commonwealth. This initiative once implemented will form the basis for a national framework for all fraud investigation.[240]

The Committee supports this attempt to develop a national framework for the investigation of fraud. It is hoped that, once developed, it will be adopted by all agencies around the country that are involved in such investigations.

Recommendation

36. The Committee supports the attempt by the Australian Institute of Professional Investigators (Victorian Chapter) and the Victoria Police Major Fraud Investigation Division to draft a set of policy standards to form the basis for a national framework for all fraud investigation.

Internal investigations

While allegations of fraud may eventually be investigated by the police, it is not uncommon for public or private sector organisations to conduct their own investigations, either in full or in part. There may be a number of reasons for carrying out such internal investigations. An organisation may, for example, only have a suspicion of fraud and may wish to confirm that it has indeed taken place. Alternatively, it may know of some fraudulent conduct that has been committed, but wants to discover the precise extent of the fraud.[241] Organisations will generally wish to know exactly what has occurred, so that they can prevent such incidents from occurring again, and perhaps recover any funds that are missing.

The power for public sector organisations to investigate fraudulent misconduct is contained in section 57 of the *Financial Management Act 1994* (Vic). In part, that section provides:

> (2) An officer who, by misconduct or by performing any duties in a grossly negligent manner, causes or contributes to a loss or deficiency in public

240 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

241 Mr Peter Zdjelar, Director, Fraud Prevention and Control, Australian Taxation Office, in conversation with the Committee, Canberra, 24 June 2003.

money or the loss or destruction of or damage to other property of the State is liable to pay to the State an amount equal to the amount of the loss or deficiency or the value of the property lost or destroyed.

(3) If an accountable officer, or the chief finance and accounting officer, of an authority is of the opinion that an officer of the authority may be liable for a loss, deficiency, destruction or damage under sub-section (2), the accountable officer or chief finance and accounting officer may direct that an investigation be held.

(4) An investigation for the purposes of sub-section (3) must be conducted in accordance with, and by a person appointed under, the regulations.

(5) After considering the report of an investigation under this section, the accountable officer or chief finance and accounting officer must determine whether or not to seek to recover an amount specified in the report of the investigation from the officer.

Private sector organisations can also conduct such investigations. Any investigations conducted will obviously need to comply with relevant legal requirements.

To conduct such investigations, organisations may either retain their own in-house investigators or engage specialised fraud investigators from the private sector. Accounting firms such as KPMG or Arthur Andersen are often hired to conduct such investigations.[242] Their roles may differ, depending on the needs of the organisation. For example, where there is limited information about the matter in question, their role may simply be to determine whether there is sufficient evidence to justify referring the matter for criminal investigation. Where more information is readily available, such investigators may conduct the entire investigation, handing the matter over to the police for prosecution. This is a common response to fraud in the Australian insurance industry.

Such investigations may be of significant value, both to the organisation and the community as a whole. From an organisation's perspective, they will have full control over the investigation, including its timing.[243] This may be important, given potential delays that could arise if the organisation were to rely solely on the police to conduct the investigation (see below). It will enable the organisation to rapidly respond to any misconduct discovered by both disciplining the person(s) involved and taking steps to prevent the recurrence of such behaviour.

From the community's perspective, such investigations may also be worthwhile, as they can reduce the burden placed on law enforcement agencies. It would be unlikely that police forces would be able to cope if they were required to investigate all instances of suspected fraud. If private sector or public sector organisations are able to afford to conduct investigations in appropriate cases,

242 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

243 Ibid.

the limited police resources available can instead be spent investigating those cases in which the victim does not have such resources at their disposal.

It is important, however, to ensure that such investigations are conducted properly. There is a danger that the use of inappropriate investigative techniques can corrupt vital evidence, reducing the likelihood of obtaining a conviction, even if a crime has been committed. It may be preferable for no investigation to be conducted, than to have an investigation conducted poorly.

To address this issue, it would be useful if organisations had clear guidelines outlining exactly when investigations are to be conducted, and how such investigations are to be performed (a 'fraud response plan').[244] Such a plan could contain clear directions on:

- examination and securing of evidence on hand
- establishing the extent of the fraud
- developing an investigation strategy
- interviewing witnesses
- managing and preparing briefs of evidence for criminal, civil or internal proceedings
- liaison with in-house and external legal counsel
- liaison with law enforcement and regulatory bodies
- providing evidence to support a claim against an organisation's fidelity insurance policy (Underwood 2003, p.11).

In drafting their fraud response plans, organisations should try to ensure compliance with relevant Standards, Codes of Practice and best practice guides in the area, such as the Internet Industry Association's draft *Cybercrime Code* (see Chapter 5). In particular, the Committee recommends that public and private sector fraud control policies and investigations follow the procedures set out in the Standards Australia *Guidelines for the management of IT evidence* (Standards Australia 2003g), to ensure that electronic evidence is preserved. The use of these guidelines was encouraged by Mr Alastair MacGibbon, Director of the Australian High Tech Crime Centre, in evidence given to the Committee.[245]

The Committee recommends that a fraud response plan be incorporated into public sector fraud control policies (see Recommendation 6a). Where private sector organisations develop and implement such policies, it would desirable if they were to also contain guidance on such issues. To this end, the Committee recommends that the Victorian Fraud Information and Reporting Centre (VFIRC) promote the importance of private sector organisations specifying in

244 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

245 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

their fraud control policies the steps to be taken in investigating suspected fraud.

Recommendations

37. The Committee recommends that VFIRC promote the importance of private sector organisations specifying in their fraud control policies the steps to be taken in investigating suspected fraud.

38. The Committee recommends that public and private sector fraud control policies and investigations follow the procedures set out in the Standards Australia *Guidelines for the management of IT evidence*, to ensure that electronic evidence is preserved.

Law enforcement agency investigations

While internal investigations can be of great use in determining the precise nature and extent of fraudulent conduct, it is likely that many allegations of fraud will, at some stage, also be investigated by a law enforcement agency. This will particularly be the case if Recommendations 34b and 34f are implemented, according to which suspected frauds will have to be reported to VFIRC, with all reports being transmitted to Victoria Police for further consideration. It is therefore important to ensure that the investigation of such matters by law enforcement agencies operates effectively.

Unfortunately, the investigation of white-collar crime is not simple. The effective investigation of white-collar crime and fraud offences therefore requires considerable resources and specialised training for those involved. Where computers are used in the commission of white-collar crimes, particularly economic crimes, the difficulties of investigation are exacerbated because offenders are able to disguise their identities and activities through the use of complex electronic technologies. Anonymous remailers and encryption devices can shield offenders from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies (see Grabosky & Smith 1998). As a result, some crimes may not result in an immediate loss, with detection not taking place until some time after the crime was committed. This, of course, makes the process of investigation even more challenging.

The use of encryption, in particular, makes it difficult, and on occasions impossible, for law enforcement and other official agencies to read relevant communications. This was seen in the international investigation conducted into the 'W0nderland' group[sic]. As discussed in Chapter 4, this was a group that was involved in distributing child pornography. They used heavy encryption, which prevented law enforcement officers from obtaining evidence. In business contexts, there is a similar risk that individuals could encrypt important communications and then refuse to decrypt them unless a fee is

paid. While it may be possible to eventually decrypt such information, this could be expensive and time-consuming. In addition, much time and expense may be invested in the decryption of files that could turn out to be deliberate decoys.

The Committee also heard of the increasing use of steganography to conceal data.[246] Steganography is the process of hiding data within digital graphic files such as GIF or JPEG files. To the casual observer, only an image is present, when, in fact, other digital information is present, embedded in the data stream. It is argued that the use of steganography makes detecting and monitoring criminal activities extremely difficult for police. This technique is now being used in connection with money laundering, banking and financial records and other illegal business activities.

Other issues that may complicate the investigation of computer-based frauds are the logistics of search and seizure during real time, and the sheer volume of material in which incriminating evidence may be contained.

Specialist units and training

A number of strategies have been adopted to respond to these difficulties. One concerns the development of specific agencies to deal with complex crime. For example, as discussed above, at a national level the AHTCC has been established to try to deal with the complexities of electronic crime. The Centre has been equipped with up-to-date technological resources, and its employees provided with specialised training.

In Victoria, the investigation of large-scale, complex crimes involving fraud and dishonesty is undertaken by the Major Fraud Investigation Division (MFID) of Victoria Police. Less complex matters are investigated by local Criminal Investigation Units. The MFID is divided into six squads: an Initial Action Squad, three Major Fraud Investigation Squads, an Asset Recovery Squad and a Computer Crime Squad. It is a multidisciplinary Division, consisting of accountants, solicitors and administrative staff, as well as detectives.[247] At present it has 135 personnel, making it almost three times the size of the next largest fraud investigation agency in Australia.[248] It is also equipped with up-to-date technological resources.[249]

246 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

247 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

248 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

249 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

Recently initiatives have been taken to establish comprehensive training programs for those involved in the investigation of fraud.[250] For example, the MFID has an Economic Crime Course that is made available to all members of the MFID, other areas of Victoria Police and external investigators from the private and public sectors. The Detective Training School (DTS) course for Victoria Police detectives also contains a Fraud Module with instructors from the MFID. This module runs for just over half a day. Course participants are provided with training in initial action in fraud investigation of eCrime, credit card skimming, forensic accounting and legal consultation, as well as being taken through a case study on a major fraud investigation. Personnel from the Victoria Police Computer Crime and Asset Recovery Squads also provide training throughout the DTS course.[251]

A number of tertiary institutions have also developed courses in the area. For example, Latrobe University, in conjunction with Victoria Police, conducts a Fraud Investigators' Course (Graduate Certificate), which has been in place for five years.[252] Melbourne University Private, also in conjunction with Victoria Police, conducts an Electronic Crime Investigation Course (Graduate Certificate) which commenced in July 2003.[253] Both of these courses are open to non-police investigators, as well police (who can receive scholarships to attend). This helps to ensure that all of those involved in the investigation of fraud and forensic accounting, from both the public and private sectors, understand each other's roles and duties and conduct investigations in a co-ordinated way.

While there is currently no formal fraud or electronic crime training provided for new police recruits at the Academy, such training, at a basic level, is likely to be offered in the future.[254]

Electronic crime investigations

Specific measures have also been introduced in the area of electronic crime investigation. In particular, the large Western democracies have introduced national policy frameworks designed to address the particular complexities that arise in this area, in order to enhance electronic communication and to

250 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

251 Letter from Acting Superintendent Stephen Leane, Legal and Corporate Policy, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 27 November 2003.

252 Discussed in submissions from Mr Allen Bowles, Corporate Crime Liaison Group and Victoria Police to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, August 2002; Letter from Acting Superintendent Stephen Leane, Legal and Corporate Policy, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 27 November 2003.

253 Letter from Acting Superintendent Stephen Leane, Legal and Corporate Policy, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 27 November 2003.

254 Ibid.

facilitate the growth of electronic commerce (Braithwaite & Drahos 2000, pp.340–41). In September 1993, for example, the United States government released its National Information Infrastructure (NII) Agenda for Action. By February 1995, this policy framework had become the Global Information Infrastructure (GII). The United States policy paper entitled *A Framework for Global Electronic Commerce* was released in 1997.

Other advanced countries have taken up these kinds of initiatives globally. They have sought to liberalise the telecommunications sector globally and to harmonise regulatory measures in order to facilitate the spread of electronic commerce. In 1994 Australia introduced its information infrastructure policy entitled *Networking Australia's Future*. The National Office for the Information Economy (NOIE) was established in 1997 to co-ordinate Australian government policy on electronic commerce, online services and the Internet. NOIE aims to facilitate the move of all sectors in the Australian economy towards the use of electronic commerce, and to identify, develop and implement world leading-edge electronic commerce solutions. In particular, the NOIE seeks to develop a comprehensive labour force strategy that will facilitate rollout of electronic commerce across Australian industries, and to develop strategies to overcome impediments to the adoption of electronic commerce (NOIE 2000).

Various specialist groups have also been established in Australia to examine the security and legal issues associated with electronic commerce. The Action Group into the Law Enforcement Implications of Electronic Commerce, for example, is a cross-agency government initiative designed to assess the technical implications of electronic commerce on law enforcement. It has produced a major report entitled *Contributions to Electronic Commerce: What Law Enforcement and Revenue Agencies Can Do* (Attorney-General's Department, Australia 1999) and continues its work into all aspects of the regulation of electronic commerce.

The other major development in Australia has been the work of the Australasian Centre for Policing Research which has reviewed current law enforcement capabilities to deal with electronic crime for the Australasian Police Commissioners' Conference. Its scoping paper entitled *The Virtual Horizon: Meeting the Law Enforcement Challenges* appeared in 2000 (Australasian Centre for Policing Research 2000). This paper comprehensively documents the issues and initiatives surrounding the problems of policing electronic crime (also known as 'cybercrime'), of which electronic fraud is a major component. Subsequently an Electronic Crime Strategy was devised for 2001–03 and presented as 'the carefully considered views of law enforcement' on these issues. Its purpose was 'to provide a safer and more secure community by preventing and reducing electronic crime' (Australasian Centre for Policing Research 2001, pp.2, 3).

The objectives of the Strategy revolve around the following five focus areas.

- Prevention: to reduce the incidence and effects of electronic crime, and to undertake sound research and maintain accurate statistics on electronic crime.
- Partnerships: to establish and maintain effective working relationships with international law enforcement, government and private agencies; to promote private sector leadership, including self-regulation where possible, and practical regulation where necessary; and to develop and maintain partnerships with communities, interest groups and non-government organisations.
- Education and capability: to have access to sufficient skilled personnel to undertake all manner of electronic crime investigations; and to create a safer community by contributing to community education about electronic crime, cyber ethics and how best to avoid victimisation.
- Resources and capacity: to have the resources and the enforcement capacity available to Australasian police to respond to and investigate electronic crime.
- Regulation and legislation: to maintain a regulatory environment that is technology-neutral, that places appropriate electronic regulation responsibilities on industry, and individuals where appropriate, that allows Australasian police to carry out effective electronic investigations, and which permits the presentation of electronic evidence within the judicial system.

The framework, as articulated by the law enforcement community, represents a sound basis for responding to the problem of electronic fraud as well as the wider issues surrounding the criminal misuse of technology. Clearly, co-operative action is essential, as the Strategy emphasises:

> The challenges of electronic crime are enormous and immediate, and no agency or nation can realistically expect to deal with the problem alone (Australasian Centre for Policing Research 2001, p.3).

More recently, the re-structure of the National Crime Authority and its replacement with the Australian Crime Commission has included an initiative that enables this body to now investigate cybercrimes. The *Australian Crime Commission Act 2002* (Cth) inserts 'cybercrime' into the definition of 'serious and organised crime', giving the Commission jurisdiction to handle matters of this nature. The Commission has jurisdiction over 'fraud', as well as cybercrime, as long as these involve two or more offenders and substantial planning and or organisation; and involve, or are of a kind that ordinarily involves, the use of sophisticated methods and techniques; and are committed, or are of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and are punishable by imprisonment for a period of at least three years.

Recent events on the world stage have seen a new layer of security concerns added to the foundations of electronic commerce policy described above, led by the United States. In his Homeland Security Policy and Budget, published under the title *Securing The Homeland, Strengthening The Nation*, the President of the United States has instigated a range of measures to enhance cyberspace security, including security of financial services in both the public and private sectors. Over 130 Federal Bureau of Investigation special agents and other investigative staff are being specifically assigned to combat cybercrime and protect banking, finance, energy, transportation and other critical systems from disruption by terrorists. A multi-million dollar funding boost for university scholarships in the field of computer security was announced under the 'Cybercorps Scholarships for Service' program. Furthermore, a new federal 'Advanced Encryption Standard' was released in December 2001, and is expected to be used widely in the private sector as well as by government (United States President 2002, pp.21–3).

Law enforcement challenges

Despite such measures being taken to address some of the complexities of fraud and electronic crime, a high level of dissatisfaction with law enforcement investigations in these areas was expressed to the Committee. In particular, concerns were raised over the length of time such investigations often take, especially where they are investigated by Criminal Intelligence Units (CIUs) rather than the MFID.[255] The division of cases between the MFID and CIUs was another area of concern.[256] Often, it was submitted, cases were classified as being insufficiently complex for investigation by the MFID, but too complex for ordinary CIUs to deal with – resulting in those matters not being dealt with at all or given a low priority.

It was also brought to the Committee's attention that certain CIUs in Victoria have been reluctant to deal with matters involving complex economic crime due to a lack of resources, unsatisfactory sentencing outcomes, and the perception that the victims had failed to take preventive measures against the risk of fraud. The allocation of certain matters between specialised Divisions within Victoria Police (such as the MFID, the Organised Crime Squad, the Tactical Response Squad and the Asian Squad) was also seen as difficult, particularly where an overlap in jurisdiction is present.[257]

255 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002; Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

256 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002; Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Mr Dennis Challinger, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

257 Submission (name withheld) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

Additional concerns were raised about the skill level of police working in the area. Economic crime is quite different from other types of crime, and many of the usual investigatory techniques are not applicable. While specific training is provided to police who come to work in the MFID, it was noted that it takes time to develop the necessary skills. By the time such skills have been developed, officers will often be ready to transfer to other parts of Victoria Police, requiring new officers to be trained. This is seen to be a relatively inefficient system.[258]

It was suggested in one submission that 'dissatisfaction with police investigations of these sorts of offences is primarily responsible for non-reporting of incidents'.[259] It is therefore vital that the problems outlined above be addressed.

Resources and training

A number of submissions made to the Committee suggested that many of the issues outlined above result from under-resourcing of law enforcement agencies, a problem evident throughout Australia.[260] It was suggested that a number of reported cases each year simply cannot be investigated because law enforcement agencies lack the personnel required to respond in a timely way to the increasing number of cases coming to their attention. In Victoria, despite the MFID having the most staff of all state and territory police services, there remains a need for additional resources in order to reduce the time taken to investigate these serious, complex, and time-consuming allegations involving fraud and deception.[261]

The current level of resourcing available to Victoria Police in this area also means that those non-sworn officers who have developed the special skills needed for investigation in this area cannot be offered salaries commensurate with those that are available in the private sector. This can lead to a high turnover of employees with the necessary skills, as they seek employment elsewhere.

Additional funds are also needed to ensure that police have available to them the latest tools and computer equipment necessary for investigating economic crime.[262] For example, one submission discussed the increasing use of steganography to commit such crimes (see above), noting that law enforcement

258 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

259 Submission (name withheld) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

260 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

261 Submission (name withheld) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

262 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

agencies need to be provided with 'tools, techniques, equipment, and training to keep abreast of [steganography] in order to maintain a capability to respond to this electronic crime threat'.[263]

The need for ongoing training was also identified in evidence given to the Committee.[264] Such resources should be used to help retain personnel who have developed particular experience in, or aptitude for, fraud investigation.[265]

As discussed above, the need for additional resources is not peculiar to Victoria Police. In conversations with the Western Australian Police, it was noted that a similar need had been identified in Western Australia. As a result, special government funding has been granted to the Commercial Crime Division of the Western Australia Police. It is provided with $500,000 in its recurrent budget each year, to be used on training, technology, marketing and travel.[266]

In light of the increasing incidence of fraud-related offences, and the special needs of those involved in such investigations, the Committee recommends that extra resources be provided to Victoria Police. It is hoped that increasing resources would help to generate confidence in the ability of Victoria Police to investigate and prosecute allegations of white-collar crime.

One use that these resources should be put towards is the provision of additional fraud-related training. For all police, especially those working in the area, fraud-related training would help develop necessary skills. The need for such training was identified in evidence given to the Committee.[267] These resources should also be used to help retain personnel who have developed particular experience in fraud or who have an aptitude for fraud work and are computer literate.[268] Such resources could also be used to purchase the technologies necessary to combat economic crime, including computer-related crime.

Potential solutions

Problems of investigating fraud and electronic crime raise complex and often intractable problems for governments. The Committee heard a number of ideas from those with whom it spoke concerning novel strategies for improving polic-

263 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

264 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

265 Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre (AUSTRAC) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

266 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

267 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

268 Submission from Mr Neil Jensen, Australian Transaction Reports and Analysis Centre (AUSTRAC) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

ing in this area. Some that have been tried successfully in other countries cannot be directly transferred to the Australian environment, while other ideas could be adopted without difficulty.

A dedicated serious fraud office

One possible way in which to address these issues would be to establish a separate agency specifically designed to investigate fraud-related matters. A number of such agencies exist around the world. In the United Kingdom, for example, the Serious Fraud Office was established in 1988. It is an independent government department that investigates and prosecutes serious or complex fraud.[269] A similar organisation exists in New Zealand (the New Zealand Serious Fraud Office). The European Union also established the European Anti-Fraud Office (OLAF) in 1999, 'to fight fraud against the [European] Community's financial interests'.[270]

While such agencies differ in their specific structures, they each operate by using multidisciplinary teams that include police investigators, forensic accountants and people with computer expertise. They will generally be given broad-ranging investigatory powers, including the power to compel organisations to provide them with particular documents. In the case of the New Zealand Serious Fraud Office, they also have the power to prosecute. This allows the one team to stay with a matter from start to finish.[271]

Such agencies are seen to be advantageous for a number of reasons. As noted above, fraud investigations can be particularly complex. In addition, they differ from most other criminal investigations in that they are generally about documentary evidence, rather than being people-based. As such, they require a different investigation technique and mindset.[272] It is arguable that establishing an agency dedicated to such investigations can best provide this. Such an agency could employ those with the necessary skills and a desire to work in the area. Hopefully such employees could be retained, addressing the problem outlined above of police learning the necessary skills but then transferring to other parts of the police force.

As a separate agency, there would not be a problem with police being taken off fraud investigations to work on matters sometimes considered more 'important', such as murder or rape investigations, as often happens under the current system.[273] This redistribution of staff resources is thought to be one of the reasons for the long delays often encountered in fraud investigations.

269 http://www.sfo.gov.uk/about/about.asp.

270 http://www.europarl.eu.int/comparl/libe/elsj/zoom_in/24_en.htm.

271 Mr David Bradshaw, New Zealand Serious Fraud Office, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

272 Ibid.

273 Ibid.

Despite such potential advantages, the Committee is not in favour of the creation of a separate fraud investigatory agency within Victoria or Australia. While such a body may be advantageous at a national level, the Committee is aware that the Australian federal systems would make such a proposal constitutionally difficult to achieve. The Committee is also of the view that state-based offences are most appropriately investigated by state police services. Victoria Police already has an existing infrastructure, both in terms of personnel and powers of investigation. The Committee is reluctant to create an additional body, which may need to be given significant investigatory powers, such as powers of surveillance, arrest and search and seizure. It would be preferable to focus instead on ways in which to resolve problems within the existing infrastructure.

In addition, fraud-related crimes are often part of a larger context, which can involve an assortment of different offences. For example, they are often related to money laundering, drug-related offences and even terrorism. Rather than having separate agencies investigate specific elements, it would be preferable to have one agency (Victoria Police) with the power to look at the overall picture throughout Victoria. The Committee therefore recommends that primary responsibility for the investigation of fraud in Victoria remain with Victoria Police.

Low-value complex fraud

Another idea is to establish a dedicated agency within Victoria Police to handle low-value but complex fraud that often can be overlooked because it is neither serious enough to warrant immediate investigation by the MFID nor simple enough to be dealt with easily by CIUs.

These low-value, complex frauds may not, on the surface, appear to be a high priority. A somewhat complicated scheme that defrauds consumers of a few hundred dollars may seem insignificant compared with a major corporate fraud that results in a loss of millions of dollars. If such a scheme is well organised, however, and manages to defraud thousands of people of a few hundred dollars each, its significance becomes more apparent. Unfortunately, victims of such crimes often do not have the resources to investigate the matter themselves, as do many victims of large-scale corporate frauds.

These factors have led the Corporate Crime Liaison Group (as it then was) to argue that the investigation of such matters should be a priority.[274] The Committee agrees. Unfortunately, such matters do not sit neatly within the current structure of Victoria Police. The Committee therefore recommends the establishment of a new sub-division of Victoria Police that can deal with complex financial crimes that involve small-value losses. Such crimes do not fall within the scope of the MFID, but are also unable to be handled by CIUs

274 Submission from Mr Allen Bowles, Corporate Crime Liaison Group to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

owing to their complexity or the nature of the investigatory expertise required. Additional resources should be provided to help establish this sub-division.

The Committee further recommends that clear guidelines be developed to help determine when matters will be examined by this new sub-division, the MFID, CIUs, or other parts of Victoria Police, and when Victoria police should work in conjunction with other state or national agencies or other bodies. Such guidelines would be a useful tool in ensuring that no matters are overlooked. Once established, these guidelines should be provided to VFIRC to help it in making recommendations as to which is the most appropriate body to investigate the reports it has received (see Chapter 8).

Partnership policing

It is unlikely, even with the provision of additional resources, that the police will be able to adequately investigate all fraud-related allegations in a timely fashion. This will particularly be the case if Recommendations 34b and 34f are adopted, according to which all cases of suspected fraud must be reported to VFIRC and passed on to Victoria Police. This may significantly increase the workload of an agency that is already under-resourced.

One way in which this issue could be addressed would be through the greater use of partnership policing. This would involve police working closely with public and private sector organisations in the investigation of crime. In particular, it would involve those outside police ranks undertaking some of the investigatory processes traditionally reserved for police.

The greater use of partnership policing was suggested by a number of parties who gave evidence to the Committee.[275] Such an alliance between law enforcement agencies and the private sector was also seen as necessary by Superintendent Masters of the Major Fraud Investigation Division, who stated that 'it is imperative that private sector, financial and banking organisations proactively seek solutions to existing problems through strategic partnerships and active consultation with law enforcement agencies'.[276]

To some extent such policing already takes place. As noted above, some private sector organisations already undertake preliminary investigations, before handing their results over to the police. In addition, Victoria Police already engages outside experts for their specific knowledge in particular areas when necessary. One example of partnership policing was provided by Mr Andrew Tuohy of KPMG, who referred to a case in which KPMG had prepared summary

275 For example, Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003; Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

276 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

sheets for use when interviewing parties involved in the matter. These summary sheets were used by the police when conducting the interviews.[277]

There is, however, no formal structure for partnership policing in Victoria. Decisions are made on an *ad hoc* basis. This has led to some dissatisfaction from those in the private sector who wish to see more use made of partnership policing.[278] For example, in one submission to the Committee, a large corporation expressed its dissatisfaction with the response it received when it offered to assist an investigation by taking statements from witnesses and paying travel expenses for police to take statements from witnesses interstate, but these offers were not taken up.[279]

It was suggested that arrangements should be developed whereby particular allegations could be investigated by the private sector.[280] Procedures could also be developed to specify which aspects of a particular investigation could appropriately be undertaken by non-police members and which should be reserved for the police. In evidence given to the Committee, Mr Newlan from the Corporate Crime Liaison Group suggested that the CCLG could help in the development of such procedures, by liaising with the police and the private sector.[281]

In light of the increasing sophistication of many forms of fraud, as well as the lack of available resources, the Committee believes it likely that law enforcement agencies will need to engage the specialised skills of experts outside police ranks more frequently in the future. In particular, it is likely that there will be a need for law enforcement agencies to hire private computer security professionals and forensic accountants for their specialised knowledge. It would therefore be useful to develop clear guidelines about when such partnerships would be appropriate and how they would work.

The New South Wales Government identified this need for partnership policing and established a Ministerial Taskforce in 2002 to examine the issue.[282] The Business Fraud Ministerial Taskforce was headed by the chief executive officer of the State Chamber of Commerce, Margy Osmond. It comprised the Police Ministry, senior police and representatives from the private sector, including the insurance and financial sectors. Its terms of reference were:

277 Mr Andrew Tuohy, KPMG Forensic, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

278 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

279 Submission (name withheld) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

280 Submission from Mr Allen Bowles, Corporate Crime Liaison Group to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

281 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

282 The Taskforce completed its final report in September 2002.

> to identify the current problems in the investigation of fraud; prioritise fraud types on the basis of impact and difficulty for police to investigate; identify and consider current public-private partnership [PPP] models for the investigation of fraud, including workable information exchange protocols; give consideration to the relevant legal issues regarding the exchange of information; determine the desired outcomes of the PPPs; develop proposals for PPPs in fraud investigation and information exchange to be considered by the [Police Minister's Advisory Council] and develop an evaluation plan (NSW Legislative Council 2002, p.2990).

The Committee recommends the establishment of a similar task force to examine the policing of fraud in Victoria, with a particular focus on the issue of partnership policing. It should aim to develop procedures that can assist law enforcement agencies to work together with the public and private sectors to build an effective fraud response framework.

Recommendations

39a. The Committee recommends that primary responsibility for the investigation of fraud in Victoria remain with Victoria Police.

39b. The Committee recommends that additional resources be provided to Victoria Police to enable it to:

i. provide additional fraud-related training to its members;

ii. retain personnel with particular experience in fraud;

iii. purchase new technologies necessary to combat high tech crime;

iv. establish a new sub-division to deal with complex financial crimes that involve small-value losses which do not fall within the scope of the Major Fraud Investigation Division but are also unable to be handled by Criminal Intelligence Units owing to their complexity or the nature of the investigatory expertise required; and

v. develop clear guidelines to determine when matters will be examined by the new sub-division, the Major Fraud Investigation Division, Criminal Intelligence Units, or any other parts of Victoria Police, and when Victoria Police should work in conjunction with other state or national agencies or other bodies .

39c. The Committee recommends that a Ministerial Task Force be established to examine the policing of fraud, with a particular focus on the issue of partnership policing, namely the development of procedures that can assist law enforcement agencies to work together with the public and private sectors to build an effective fraud response framework.

Conclusion

The investigation of fraud and electronic crime is becoming increasingly difficult, as the nature of such crime becomes more sophisticated. This has led to a need for greater co-operation between all parties working in the area. In particular, the investigatory skills of the police need to be combined with the specialist knowledge of forensic accountants and computer security professionals, if an effective investigation framework is to be developed. Such a framework is necessary if evidence of such crimes is to be properly uncovered, enabling successful prosecutions to be undertaken. The prosecution and sentencing of those who have committed such crimes is examined in the following chapter.

10. Legislative and Judicial Responses

Introduction

Chapter 9 discussed the challenges that face law enforcement agencies in investigating fraud and electronic commerce-related offences. This chapter now considers the adequacy of the law and the courts in dealing with economic crimes. As with other sections of this Report, many of the challenges relate to the need for harmonised laws and procedures throughout Australia, and also internationally, and the Committee is keenly aware of the need for Victorian law and policy to reflect best practice globally.

Criminal proceedings for theft or deception aim at punishing the offender in the retributive sense, denouncing the conduct in question, and preventing further offending by deterring the individual from engaging in similar conduct in the future. They also seek to deter others in the community from offending by making an example of the individual in question (Walker 1991). In serious cases, guilt is determined by a jury and criminal compensation may be awarded in certain circumstances.

The penalties that are available to a judge in sentencing an offender include imprisonment, fines, community-based orders and various forms of conditional and supervised release. The extent to which such sanctions are appropriate and effective in deterring unprofessional conduct by so-called white-collar offenders is hotly debated and many have argued that other sanctions could be more appropriate, such as adverse publicity, financial penalties, or compulsory training in ethics and professional conduct (Grabosky 1995). Arguably, fines are a better sanction for white-collar offenders as they more readily match the nature of the conduct with the penalty imposed and avoid the unintended consequences of custodial sanctions (see 'Sentencing' below).

This chapter discusses questions of policy and legislative reform by first considering various non-criminal justice responses that are available to victims of fraud, including civil action and professional disciplinary action, and then examining the substantive laws that are relevant to the prosecution of fraud and electronic commerce in Victoria. It then reviews some of the jurisdictional and procedural issues before considering court procedures and questions of

sentencing. Given that fraud entails some of the most complex and intractable forensic issues known to the criminal justice system, the solutions are unlikely to be simple. In conversation with the Committee, a representative from the National Office of the Information Economy observed that regulation in the online environment was similar to regulation of the oceans as all nations have an interest in the outcome and all must agree on any proposed reforms.[283] Just as the reform of the law of the sea has taken decades to be agreed upon, so the reform of cyberspace will take time (hopefully less than in the case of the law of the sea). It is hoped that the United Nations will have a role to play in achieving agreement on the appropriate responses.

Fortunately many reforms have already been undertaken and some effective solutions reached, which have improved the operation of criminal justice agencies not only in cases of economic crime and cybercrime but also in other types of crime as well. In this sense, technology has provided an impetus to reform that has led to legislative change taking place much more quickly than in some other areas in the past. Of course, speedy reforms are not always the best, and only with time will some of the practical problems begin to emerge.

What avenues of redress, then, are available to those victimised by financial criminals?

Civil remedies

Ultimately, the decision to mobilise the law, and the choice of remedy, will require that law enforcement and regulatory authorities consider a range of factors, such as the likelihood of success, the cost involved, and the public interest. In the current climate of resource constraints across the public sector, the availability of private remedies and the capacity of victims to recover their losses through private litigation may also be considered. To the extent that private parties have the resources and the capacity to pursue their own remedies, the limited resources of the state may be reserved for those situations where they are most sorely needed.

As an alternative, or in addition to instituting criminal action, victims of fraud may also commence civil proceedings for damages in negligence, trespass or breach of contract, although the legal principles which apply in this area are by no means settled (see Law Commission, New Zealand 1998, Chapter 4). Traditionally fraud was regulated principally through civil action with the use of the criminal law as a regulatory strategy being a relatively new invention, at least in the history of the common law (see Page 1997 for a history of the legal regulation of fraud). Today the civil consequences of fraud continue to have widespread importance; clearly, it is beyond the capacities of police and other regulatory agencies to prosecute every allegation of fraud that comes to their attention.

283 Mr Keith Besgrove, Chief General Manager, Regulation & Analysis, Group, National Office for Information Economy, in conversation with the Committee, Canberra, 24 June 2003.

Civil action provides a financial sum to successful claimants, which aims to place them in the same position they would have been in had the wrongful act not taken place. Normally an award of damages is aimed at compensation rather than punishment, although in rare instances exemplary or punitive damages may be awarded to make an example of the defendant with a view to deterring similar conduct in the future. Damages are assessed by a jury that hears evidence presented by experts for both the plaintiff and the defendant in an adversarial setting.

The question that arises is when is it appropriate for civil action to be taken in preference to criminal proceedings. In the case of serious financial crimes perpetrated against corporations, business considerations may result in criminal action being seen as simply not cost-effective, particularly where the offence may involve elements of complexity or cross-border conduct that will inevitably lead to a lengthy and costly trial. Where the accused has some ability to pay compensation, a rational business choice would be to take civil proceedings instead of criminal action – even if that means that any deterrent effects are negated or minimised.

In the case of public sector agencies, however, criminal action is seen as being a necessary response to the misappropriation of public funds. If civil action is taken without involving the police, the importance of the matter may be undermined and that accountability for public funds would be lessened.

It is for this reason that the Committee has recommended that there should be a mandatory requirement on victims to report *serious* financial crimes to the police for investigation. The option of taking civil action would remain open, but at least with such crimes the possibility of achieving deterrent effects and denunciation of the conduct would be available.

Professional regulation

Victims of financial crimes may also lodge complaints with statutory licensing authorities in cases where fraud is alleged to have been perpetrated by certain professionals. Although the members of the oldest professions are statutorily recognised and registered, some professionals, including accountants, are not covered by existing registration authorities and thus are not subject to any internal professional disciplinary controls other than the potential loss of membership of a professional association. Where misconduct occurs in such situations, the victim will have recourse only to criminal and civil action or, in some cases, to alternative dispute resolution services offered by certain consumer agencies.

Registration bodies such as professional boards are set up to protect members of the public by providing for the registration of practitioners, such as the Board established under s.1(a) of the *Medical Practice Act 1994* (Vic). Boards are under a legal duty to investigate complaints that are made, and where allegations are proved the registration of the practitioner may be restricted in some way or

removed. Disciplinary action is not intended to be retributive, but rather is designed to maintain acceptable standards of practice in the profession (see Smith 1994). The one exception to this exists where boards have a limited jurisdiction to impose fines which are exclusively intended to be punitive and to act as a deterrent, such as in the *Medical Practice Act 1994* (Vic) s.50(2)(f).

Some boards may also require practitioners to undergo counselling or further education in order to remedy any deficiencies in their professional skills. The effect of disciplinary action may also be to declare standards of acceptable conduct for the rest of the profession, although this is obviously dependent upon the extent to which decisions in disciplinary cases are disseminated to registered practitioners (Smith 1993).

Registration boards are predominantly composed of senior, experienced members of the profession in question, although in recent years the proportion of non-medically qualified lay-members is increasing substantially, such that most boards, at least in the health care professions, now have 25 per cent of their membership non-medically qualified (Smith 1994). Formal proceedings are now usually open to the public and they are adversarial and conducted with legal representation (Smith 1991).

Proportionally, there are few complaints made to disciplinary bodies each year. In Victoria, for example, approximately 2,300 complaints are made each year concerning the conduct of solicitors (Neville 2000). These relate to problems of delay, poor attitude, over-charging, and misappropriation of funds. In 1999, 21 practitioners were referred to the profession's tribunal for a disciplinary hearing. Of those cases, 12 had their practising certificates cancelled or reduced, and were fined; seven were fined without restrictions being placed on the practising certificate; and two cases were dismissed. On average, six practices a year are taken over by the Law Institute in Victoria because of trust account defalcations, which represents approximately 2 per cent of the 3,411 solicitors authorised to handle trust funds in the state. Most cases related to misuse of investment funds, although since controls have been placed on solicitors' mortgage practice these cases have reduced substantially (Neville 2000).

In medicine, approximately 1,000 complaints are made each year to the New South Wales Medical Board which regulates the conduct of approximately 22,000 registered medical practitioners in that state (4.5%) (Dix 2002). In Victoria, between 2000/01 and 2001/02, the number of complaints made to the Medical Practitioners Board of Victoria rose some 43 per cent, from 401 to 573. Given that there are more than 17,000 registered medical practitioners in Victoria, this number is a relatively low proportion. The range of complaints received in 2001/02 remained broadly consistent with the previous year, with the largest percentage (42%) relating to clinical care, standard of practice and poor outcomes. There was an increase in complaints about medical practitioners' conduct or behaviour and fewer about sexual misconduct (Medical Practitioners Board of Victoria 2002).

Within the nursing profession in 1995/96, approximately 600 nurses were reported to regulatory authorities throughout Australia, at a time when there were approximately 265,000 registered nurses (making the proportion of complaints to the total numbers of nurses 0.2 per cent) (Fletcher 1998).

During this Inquiry the Committee received evidence that called for more effective professional regulation of members of the accounting profession including financial advisers.[284] Although the vast majority of accounting professionals act honestly and in accordance with high professional standards, there is the potential for extensive hardship to be inflicted where accounting professionals abuse their trust by stealing client funds.

At present, the regulation of accounting professionals is undertaken in a largely informal way through the membership of professional associations such as the Institute of Chartered Accountants in Australia and the Australian Society of Certified Practising Accountants. Where members of these bodies act unprofessionally or criminally, there is the possibility of membership being withdrawn. The Committee believes, however, that a more stringent regulatory mechanism would be appropriate with the possibility of complete prohibition from professional practice being imposed for the most severe forms of professional misconduct, as well as financial penalties being imposed by a statutory panel, such as occurs in the case of lawyers and doctors.

Recent reforms to the regulation of the financial services industry introduced by the *Financial Services Reform Act 2001* (Cth) will result in a requirement that all financial planners in Australia are registered by 11 March 2004. However, the Committee heard concerns that these licensing regulations could be circumvented by individuals who are either unlicensed or prohibited from acting as financial planners continuing their activities in other ways that would not technically amount to the provision of financial planning advice.[285] The Committee suggests that such any such conduct which could circumvent the effectiveness of ASICs regulatory function be further investigated and rectified.

284 Mr Tim Farrelly, Independent Researcher, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

285 Ibid.

Recommendations

40a. The Committee recommends that an inquiry be conducted into the introduction of a statutory system for the professional regulation and registration of accountants, financial advisers and other financial consultants (such as mortgage brokers) who practise in Victoria, with a view to determining standards for admission to practise, and procedures for restriction of registration on proof of professional misconduct. The Committee recommends that legislation governing other statutorily recognised professions in Victoria be used as a model.

40b. The Committee recommends that action be taken by the Australian Securities and Investments Commission to ensure that individuals who are prohibited from practising in the financial services industry are unable to circumvent such action by continuing to practise in other advisory roles.

Mediated professional action

In recent years many professionals have been made more accountable through the introduction of independent complaint-handling authorities. These bodies operate as a form of coerced self-regulation, or what Johnson (1972) has called 'mediated professionalism'.

In Victoria, for example, the legal profession was subject to substantial reform with the introduction of the *Legal Practice Act 1996* (Vic), which ended its monopoly over the regulation of the profession. Among other reforms, the legislation introduced a Legal Practice Board, a Legal Ombudsman, and a Legal Professional Tribunal to regulate the activities of legal practitioners. The legislation made the Law Institute of Victoria a Recognised Professional Association and also made membership voluntary.

In 2003, an independent review of the legal profession's regulatory structure in Victoria recommended the establishment of a new Legal Practice Board to replace the functions currently undertaken by the Law Institute of Victoria, the Legal Ombudsman and the existing Legal Practice Board (Shiel 2003). The establishment of an independent regulatory agency was seen as leading to improved outcomes and reduced costs which currently amount to $11.9 million annually. In 2001/02 the Law Institute of Victoria received 2,849 complaints concerning the conduct of solicitors in Victoria, mainly relating to costs, failure to return clients' calls, excessive delay and negligence (Shiel 2003).

In New South Wales, the Office of the Legal Services Commissioner has also made the handling of complaints substantially more consumer-oriented (see Parker 1997, p.16).

In relation to health care, all jurisdictions in Australia have Health Complaints Commissioners whose functions include the resolution of disputes between health providers and patients arising out of the provision of health services. Commissioners are required to investigate complaints and may resolve them by

conciliation, which simply means encouraging a settlement of the complaint by holding informal discussions with the health provider and the patient. Conciliators often do not have training in the profession in question, although they may be officially qualified as conciliators. Where necessary, they will seek expert assistance from relevant trained professionals. Complaints may be resolved by extracting an explanation and apology from the health provider or by the health provider's defence organisation paying a sum of money to the complainant. If conciliation fails, the Commissioner may refer the complaint to a Registration Board for disciplinary action (see *Health Services (Conciliation and Review) Act 1987* (Vic.)).

There are also prospects for certain cases of alleged fraud, even across borders, to be resolved through the provision of alternative dispute resolution services online (see, for instance, Consumers International 2000). Of course, those perpetrating intentional frauds are no more likely to submit voluntarily to this process than they are to give themselves up to law enforcement authorities. However, these extra-legal avenues of problem solving across borders are generally much cheaper and more efficient than public investigations, and are likely to help reduce the number of cases that would otherwise be pursued by authorities in the criminal courts.

Substantive laws

At present in Australia each jurisdiction has its own laws and rules that regulate business and professional activities. These emanate from all levels of government, professional bodies, business organisations and many other bodies. Many are complex, unclear, and contradictory and impede the successful investigation and prosecution of many white-collar crimes. Any policy or legislative response to the challenges presented by new technologies should avoid complicating matters further and attempts should be made to harmonise legal reforms across Australia as well as internationally.

This section reviews the current law and policy in relation to the themes of fraud and dishonesty, computer crime, electronic commerce, consumer protection and information privacy, and discusses relevant proposals for reform.

Fraud and dishonesty

As noted in Chapter 1, the law concerning fraud offences in Australia is a complex patchwork of common law and statute, pieced together and handed down through history.

> The nine jurisdictions operate under nine sets of laws which adopt fundamentally different criteria ... Even the definitions of the basic theft offence are each fundamentally different from one another (Model Criminal Code Officers Committee 1995, p.ii).

As crime increases in the borderless online environment, the lack of uniformity of the laws concerning dishonesty across Australia is increasingly a cause for concern. Even allowing for the inherent complexities of a category of offences that ultimately depend on a person's state of mind, the sheer volume of law in this area serves only to hamper law enforcement efforts. The leading Australian textbook on theft states:

> There is no reason why conduct which is criminally dishonest should not be conceived and defined uniformly throughout Australia. Certainly there is no justification for continued toleration of the complexity and extreme technicality of the common law in this area (Williams 1999a, p.1).

One of the most important national policy goals in recent years has been to clarify the legal rules that govern fraud offences. This would not only help to maximise the possibility of offenders being prosecuted successfully, but would also facilitate the collection of uniform crime statistics throughout the nation by police. Moreover, in an age when most fraud offences are carried out through the use of computers in some way or other, the definition of fraud, and particularly its geographical scope, needs to be drafted in technology-neutral terms ensuring that even the most sophisticated offenders may be charged under the available offences, the crucial first step in an effective system of criminal prosecution.

Federal law

The Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General has addressed the problem of harmonising laws in Australia. The Australian government has enacted legislation to establish uniform rules governing offences of theft and fraud with the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*, which received assent on 24 November 2000 and commenced on 24 May 2001.

Relevant offences introduced into the *Criminal Code Act 1995* include obtaining property or a financial advantage by deception (Division 134), offences involving fraudulent conduct (Division 135), forgery (Division 144) and falsification (Division 145).

In addition to the obtaining offences (ss.134.1 and 134.2), which closely resemble the equivalent Victorian *Crimes Act 1958* provisions, the 'general dishonesty' offence in section 135.1 provides a maximum penalty of five years' imprisonment 'where a person does anything with the intention of dishonestly obtaining a gain from, or causing a loss to, the Commonwealth'.

Section 135.4 makes it an offence to conspire with another person to commit an act with the intention of dishonestly obtaining a gain from, or causing a loss to, the Commonwealth, although in this case the maximum penalty is 10 years' imprisonment.

The offences of forgery (s.144.1), using a forged document (s.145.1) and falsification of documents (s.145.4) provide penalties of up to 10 years'

imprisonment for the first two offences, and up to seven years for the third. They also explicitly apply to deceptions perpetrated against computers as well as those against human beings. This goes towards dealing with the problem that has occurred in judicial interpretation of deception offences in English law. A recent publication of the Law Commission in the United Kingdom stated that: 'It now appears to be settled law that a deceit can only be practised on a human mind, although there is little direct authority on the point' (Law Commission 1999, p.109).

Victorian law

In Victoria, the central dishonesty offences are found in the *Crimes Act 1958* (Vic), being theft (s.72), obtaining property by deception (s.81) and obtaining financial advantage by deception (s.82). When these provisions were introduced, based on the English *Crimes Act 1968*, they represented a significant departure from the centuries-old common law theft. While the ACT and the Northern Territory each adopted provisions based on the Victorian model in the mid-1980s, each of the other states and territories and the Commonwealth maintain separate and distinct criminal laws in this area.

Due to further reforms introduced by the *Crimes (Computers) Act 1988* (Vic), it became possible to prosecute certain of these offences when committed using computers. In section 81, deception came to include deception of a computer system or machine; section 83A was added to make the falsification of documents an offence; and a new section 80A enabled any of the offences contained in sections 81–87 to be prosecuted if a 'real and substantial link with Victoria' could be established.

Despite the fact that Victoria enjoys a relatively modern legal framework regarding dishonesty offences, the influence of ancient common law principles continues, and the strain upon it in these fast-moving times remains apparent (see Definitional issues – Fraud and dishonesty in Chapter 1). As the Model Criminal Code Officers Committee observed:

> Since the early part of the industrial revolution in the eighteenth century, judges and legislatures have been struggling to adapt the law of larceny to the needs of societies with more and more complex and abstract notions of property rights (Model Criminal Code Officers Committee 1995, p.1).

The common law offence of larceny, which prevailed in Victoria until the reforms of 1973, proscribed the taking of physical objects, or 'tangibles'.

Today the ambit of the law takes in not only tangible but also intangible property. However, the content of the latter category is problematic, particularly with respect to crimes committed electronically. 'Information technology creates new products, new capabilities, and new commercial property that challenge ancient assumptions in our law' (Lipton 1998, p.56). In an age in which it has become trite to assert that information is the essential source of value, trade secrets and confidential information are excluded from the category

of intangible property. In the eyes of the law they are literally incapable of being stolen. For example, in the case of *Oxford* v *Moss* ((1978) 68 Cr App R 183), a university student was acquitted of theft of intangible property where the item in question was a proof of an examination paper (see generally Grabosky, Smith & Dempsey 2001).

Fisse has pointed out that 'in failing to protect this type of property the supposedly modern law of theft is open to the criticism that it is already archaic' (1990, p.292). A further difficulty associated with treating information under offences of theft or obtaining property by deception is that, unlike tangibles, information can be taken without depriving the holder of it, which is an essential element of both offences (see Hughes 1989, p.507). The destruction, copying, or holding to ransom of valuable information accessed by fraudulent means are significant risks associated with electronic commerce. One simple example is the taking of credit card information, a preparatory step towards more serious offences, which might usefully be criminalised in its own right.

However, it has been argued that some of the most deleterious effects of this exclusion of information from the definition of property could be remedied quite simply. If property were defined to include 'computer data', this would cover many of the gaps currently left by the theft and 'obtaining property by deception' offences while avoiding the criminalisation of all theft of 'information', which would probably go too far (McConvill 2001).

It is clear that electronic transactions are not uniquely susceptible to unscrupulous manipulation. The misuse of paper cheques has given rise to a substantial body of case law itself over the years. As recently as 1997 the Victorian Supreme Court was required to rule on whether cheques qualified as property 'belonging to another' under the section 81 offence of obtaining property by deception (R. v *Parsons*, Court of Criminal Appeal, Supreme Court of Victoria, 24 October 1997). If paper cheques continue to create legal issues after so many years, even greater challenges should be anticipated as various forms of electronic funds transfer and digital payment systems become more widespread.

An illustration of the kinds of difficulties raised by new technologies occurred within one week of the September 11 disaster when Internet users in Australia began to receive requests for donations from bogus charities purporting to seek relief funding for the disaster's victims (Consumer Affairs Victoria 2001b). Funds gathered using such a pretext and then put to other uses would clearly involve 'obtaining a financial advantage by deception', although locating and prosecuting those responsible may well prove to be impossible (see 'Cross-border issues' below).

As can be seen from the extensive list of offences presented in Appendix C, the Victorian law in this area is by no means simple. There are many technical legal problems of construction for offences turning on the mental element of dishonesty. In the English Act, 'dishonestly' was left undefined deliberately because

it was felt that dishonesty was 'something which laymen can easily recognise when they see it' (Waller & Williams 1997 para. 8.52). The test that emerged in English cases of *Feely* ([1973] 1 QB 530) and *Ghosh* ([1982] 2 All ER 689) required first that the defendant's conduct was dishonest according to the ordinary standards of reasonable people, and second that the defendant realised this. In contrast, the first major Victorian decision on its own version of the legislation, *Salvo* ([1980] VR 401; (1979) 5 A Crim R 1), held dishonesty to be a matter for precise legal definition, not for common interpretation by juries. It was submitted to the Committee that in the interest of achieving national harmonisation of dishonesty offences, Victoria's approach should be reformed.[286]

Although the Committee was told that the Victorian law relating to theft and dishonesty is fairly adequate to enable most fraud offences to be prosecuted effectively,[287] a number of specific issues were identified that could require further investigation.

Reform suggestions

Victoria Police submitted that the offence of 'Make False Document and Use False Document' in sections 83A(1) and (2) *Crimes Act 1958* should be amended to change the intention element of the offence from 'to the prejudice of another' to 'to the benefit of the defendants' as the existing provision has caused problems in previous prosecutions.[288] In New South Wales, for example, the requirement for prejudice is seen to be increasingly difficult as it is necessary to establish that the false document in question 'told a lie about itself'. As an alternative it was suggested that the legislation could simply state: 'A person shall not dishonestly make/use a document which he knows to be false'.[289]

The Committee also heard discussion concerning the desirability of enacting a general dishonesty offence in Victoria. Such a provision would, arguably, eliminate the need for specific offences such as theft, obtaining property by deception or obtaining a financial advantage by deception. The concept was strongly supported by Victoria Police[290] and has been advocated by others interstate and overseas (eg. Page 1997). It is exemplified in section 135.1 of the *Criminal Code Act 1995* (Cth), discussed below. In Queensland the Committee heard that the relevant provision allows a person who has been

286 Mr Matthew Goode, Managing Solicitor, Policy and Law Section, Attorney-General's Department, in conversation with the Committee, Adelaide, 3 October 2003.

287 Mr Paul Coghlan QC, Director of Public Prosecutions, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

288 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

289 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

290 Ibid.

misappropriating funds for many years to be prosecuted with the use of a single count as opposed to numerous separate counts for individual amounts that are alleged to have been stolen. The Director of Public Prosecutions in Queensland told the Committee that this could reduce trial time and expense, where some counts are admitted and others disputed.[291] The Committee is supportive of this idea but only in so far as it would promote harmonisation of offences throughout Australia, as recommended by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (1995). The recommendation was that the Model Criminal Code should contain the following provision, which the current Committee believes would be sufficient:

> A person may be convicted of theft of all or any part of a general deficiency in money or other property even though the deficiency is made up of any number of particular sums of money or items of other property that were appropriated over a period of time (1995, p.344).

The Committee was also alerted to a number of other perceived deficiencies in current Victorian law. Victoria Police held the view that the definition of 'property' in section 71 *Crimes Act 1958* should be amended to ensure that intellectual property was included.[292] This, it was submitted, would assist in prosecuting infringements of intellectual property rights under state law including instances in which information such as bank account numbers have been used without authority, although most intellectual property infringements would be prosecuted under the *Copyright Act 1968* (Cth) and *Trade Marks Act 1995* (Cth) and the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General elected to deal with theft of data under the revised computer damage legislation (see below).

It was also submitted that Victorian law could be amended to enable prosecutions of company officers and employees who jointly misappropriate funds from their own company, which has been problematic in the past (see R. v *Roffel* [1985] VR 511; see also R. v *Jenkins* [2002] VSCA 224). It was also argued that the law should be clarified to ensure that theft from pooled funds, such as Superannuation Funds, can be prosecuted.[293]

Another problem raised was the difficulty of prosecuting individuals who incite dishonest conduct by publishing information on the Internet concerning the ways to perpetrate criminal activities such as credit card skimming and other acts of fraud.[294] Although the Committee is reluctant to limit free expression, and is keenly aware of the difficulties associated with

291 Ms Leanne Joy Clare, Director of Public Prosecutions for Queensland, in conversation with the Committee, Brisbane, 26 June 2003.

292 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

293 Ibid.

294 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

prohibiting content disseminated from other jurisdictions, it would be appropriate to examine ways in which particularly clear incidents of incitement to commit crimes in this way could be better regulated.

The Committee has considered these various proposals for reform, some of which clearly have merits. However, in order to support national harmonisation, the Committee suggests that Victoria refrain from undertaking specific legislative reform in the area of dishonesty, instead referring the identified problems for resolution on an Australia-wide basis.

Recommendation

41. The Committee supports continuing attempts to harmonise nationally the law relating to fraud and other dishonest conduct, including crimes involving misuse of identity and dishonest practices relating to payment cards and electronic payment systems.

42. The Committee recommends that the *Crimes Act 1958* (Vic) be amended to reflect the recommendations of the Model Criminal Code Officers Committee in relation to dishonesty offences, including fraud and forgery, as enacted in Divisions 133-137 and 143-145 of the *Criminal Code Act 1995* (Cth). In amending the law, it should be ensured that:

    i. the means of proving dishonesty in Victoria be determined according to the standards of ordinary people, and known by the accused to be dishonest according to those standards;

    ii. the definition of 'property' that can be fraudulently obtained includes intellectual property and computer data;

    iii. company directors and employees can be charged with the relevant offences where they have defrauded their own company;

    iv. people can be charged with the relevant offences where they have defrauded a pooled fund;

    v. offences are applicable to fraud committed in an online environment; and

    vi. Victorian fraud and dishonesty-related offences be able to be charged in any case where the offence was committed in Victoria, or where the victim was in Victoria at the relevant time.

43. The Committee recommends that a general fraud offence should not be established in Victoria.

Identity theft

Under Australian law the use of a false or alternate identity is not necessarily illegal. The use of an alias is, for example, common in entertainment and literary circles, while many women choose to use both their married and

unmarried names. There are, however, various laws that can be used to prosecute identity-related dishonesty.

Current Australian laws

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

In an attempt to prevent large-scale money laundering, the *Financial Transaction Reports Act 1988* (Cth) has provisions that require cash dealers (which includes many of the major financial institutions) to identify all signatories to accounts. The Act also regulates the manner in which identity must be established when accounts with financial institutions are opened. This Act creates an offence of opening an account in a false name by, for example, tendering a false passport or someone else's driver's licence or disclosing only one of two names by which a person is known. This carries a maximum penalty of two years' imprisonment (*Financial Transaction Reports Act 1988* (Cth) s.24).

It is also an offence knowingly or recklessly to make a false or misleading statement in advising a financial institution of a change of name, which carries a maximum penalty of four years' imprisonment (s.21A). Penalties also apply to cash dealers who fail to comply with reporting requirements under the Act (ss.28–34).

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

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

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

assented to on 6 May 2003 created a range of computer-based criminal offences based on the Commonwealth's *Cybercrime Act*.

Specific identity theft legislation

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) makes identity theft a crime with maximum penalties of up to 15 years' imprisonment and a maximum fine of US$250,000. It establishes that the person whose identity has been stolen is a victim who is able to seek restitution following a conviction. It also gives the Federal Trade Commission power to act as a clearinghouse for complaints, referrals, and resources for assistance for victims of identity theft. Some 47 American states now have some form of identity theft legislation, although the Federal Act is the most comprehensive.

In May 2002 the Federal Identity Theft Penalty Enhancement Bill 2002 was introduced in the United States for first reading, to amend the Federal Criminal Code to establish penalties for aggravated identity theft. This Bill was referred to the Senate Sub-Committee on Crime, Terrorism and Homeland Security on 3 June 2003. The Bill prescribes additional punishments of two years' imprisonment for using false identities in connection with felonies relating to theft from employee benefit plans and various fraud and immigration offences, in addition to the punishment provided for such felonies, and five years' imprisonment for using false identities in connection with terrorist acts, in addition to the punishment provided for such a felony. The Bill also bars probation for any person convicted of such violations.

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

In South Australia, the Criminal Law Consolidation (Identity Theft) Amendment Bill 2003 (SA) was introduced in the House of Assembly on 15 October 2003. This Bill inserts into the *Criminal Law Consolidation Act 1935* (SA) a new Part 5A that contains sections prescribing offences involving the assumption of a false identity, the use of personal identification information and the production and possession of prohibited material (Atkinson 2003). Prohibited material is defined as being anything that enables a person to assume a false identity or to exercise a right of ownership that belongs to someone else to funds, credit, information or any other financial or non-financial benefit.

The proposed new offences are:

- Assuming a false identity or falsely pretending to have particular qualifications or to be entitled to act in a particular capacity and intending to commit or help commit a serious criminal offence;
- Making use of another's personal identification information intending to commit or help commit a serious criminal offence;
- Possessing or producing material that would enable someone to assume a false identity or exercise a false right of ownership intending to use it or allow another to use it for a criminal purpose;
- Selling or giving material that would enable someone to assume a false identity or represent a false right of ownership to another person knowing it is likely to be used for a criminal purpose; and
- Possessing equipment for making material that would enable someone to assume a false identity or exercise a false right of ownership intending to use it to commit one of these offences.

The offences of identity theft also extend to corporations and to the identities of people living or dead, or fictitious identities. Because the new offences are preparatory offences, the penalties for the major offences are linked to the penalties for attempts to commit the crime intended.

The Bill defines a person's personal identification information as information used to identify the person. In the case of a natural person, this includes the person's name, address, date of birth, driver's licence, passport, biometric data, credit or debit card information and digital signature. In the case of a body corporate, personal identification information includes the corporation's name, its ABN and the number of any bank account established in the body corporate's name or of any credit card issued to the body corporate.

In order to exclude the activities of children, the Bill's provisions do not apply to the conduct of under-age persons attempting to be admitted to age-restricted venues or to purchase age-restricted items, such as cigarettes or alcohol, as the existing offences were considered sufficient to deal with these situations.

The Bill also amends the *Criminal Law (Sentencing) Act 1998* (SA) to give victims the right to obtain a certificate from a court so that they can prove that an offence has been committed against them.

The Committee received a number of submissions supportive of this type of Bill,[295] and the question arises as to whether Victoria should also enact similar legislation. Victorian law already has substantial maximum penalties available

295 Mr Matthew Goode, Managing Solicitor, Policy and Law Section, Attorney-General's Department, in conversation with the Committee, Adelaide, 3 October 2003; Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

for identity-related fraud offences, with terms of imprisonment of up to 10 years being provided for serious offences. Although the enactment of specific identity-related fraud legislation would provide a public statement that conduct of this nature is illegal and is being specifically addressed by the Victorian government, it would, arguably, achieve little in assisting in the prosecution of offences and in ensuring that convicted offenders receive appropriate sanctions. The current difficulties associated with prosecuting identity-related crimes lie not so much in legislative inadequacies as in the practical problems associated with persuading victims to report offences for investigation, and in locating suspects, many of whom may be outside Victoria.

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

One submission received by the Committee suggested that the mere possession of counterfeit or altered evidence of identity documents should be a criminal offence. [296] It was submitted to the Committee that none of the existing criminal offences in Victoria deal with preparatory acts associated with identity theft nor do they cover the following situations: using a fraudulent name without making a false document; using a fraudulent name to obtain a legitimately issued document; stealing personal information with intent to fraudulently use for gain; possession of personal information with intent to use it for gain; possessing personal information with the intention of making false documents or obtaining legitimately issued documents; accessing computer systems with intent to steal personal information for benefit or gain; or using a position of employment to steal personal information.[297] As is apparent from Appendix C-1, however, Victoria already has a number of relevant offences that could be used in this context.

It was also suggested to the Committee that an accused person should bear the burden of having to prove that possession and use of such equipment or

296 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

297 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

counterfeit documents was legitimate.[298] At present, possession of such equipment or documents could form the basis of a charge of conspiracy to defraud where two or more persons were involved in the creation or possession of false instruments, although it was submitted to the Committee that it is sometimes difficult to establish the necessary intention to defraud. However, the Committee was told that this would be a serious departure from the traditional burden of proof which operates in criminal proceedings and that this could create hardship in terms of requiring individuals to prove that they were acting honestly.[299] In view of the heavy maximum penalty that would apply, the Committee believes that the decision to reverse the burden of proof for such conduct does not seem at all reasonable or justifiable.

In view of the recommendations of the Committee (above) that support the national harmonisation of fraud and dishonesty offences, it is considered preferable to refer the question of the enactment of identity-related fraud legislation to the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (see below).

Credit card fraud

A related area concerns the desirability of enacting legislation to proscribe conduct preparatory to the commission of fraud involving payment systems, particularly relating to the misuse of credit cards and account information. The Committee received a number of submissions identifying crimes relating to the misuse of payment cards as a serious and escalating problem in Australia. Victoria Police said that credit card fraud was an increasing problem, as more and more of the population use credit cards and organised crime groups increasingly target these payment systems. To combat this, countries such as Canada, Taiwan, Hong Kong and Japan have introduced specific and stronger legislation, which has led to a decrease in the problem in those countries and, it was submitted, an increase in countries like Australia.[300] Victoria Police also estimated that card skimming in Australia had increased some 500 per cent in the past 12 months,[301] while the Regional Director of American Express saw this as its largest current fraud problem.[302]

A range of difficulties were identified in current legislation that precluded the effective prosecution of persons who manufacture credit cards

298 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003; Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

299 Mr Matthew Goode, Managing Solicitor, Policy and Law Section, Attorney-General's Department, in conversation with the Committee, Adelaide, 3 October 2003.

300 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

301 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

302 Mr Jilluck Wong, Regional Director, Fraud Prevention, American Express, in conversation with the Committee, Sydney, 25 June 2003.

fraudulently or who alter lost or stolen cards and then use them to withdraw funds. There was also said to be no offence of importing counterfeit cards or devices that could be used in connection with card skimming or other fraudulent activities.[303] In a submission to the Committee, Victoria Police argued that credit card skimming activities are currently only covered by obtaining property by deception, obtaining a financial advantage by deception, make/use false document, possess false document, and possess implement to make false document offences. It was argued that this excludes preparatory acts, such as stealing credit cards, forging or falsifying credit cards, possessing, using or trafficking in forged or falsified credit cards, possessing, using, trafficking, making or dealing in implements, devices, apparatuses or materials or things used or adapted for forging or falsifying credit cards, and possessing, obtaining, using or trafficking in credit card data or credit card numbers.[304]

In Western Australia an offence exists of 'preparation for forgery' (s.474) which proscribes the possession of anything that could be used to carry out acts of forgery with an intention to forge documents. Often, however, difficulties are encountered in providing the requisite intent.[305] In Hong Kong, legislation exists which enables offenders to be charged with possession of any article used for or in connection with the manufacture of counterfeit credit cards.[306]

As was the case in connection with identity-related fraud offences (see discussion above), a number of submissions received by the Committee suggested reversing the onus of proof, thus requiring an individual found in possession of equipment that could be used in connection with the manufacture of counterfeit credit cards to adduce evidence that the equipment was held for legitimate purposes. It was suggested that the creation of a more regulated industry in which manufacturers of plastic cards were required to be licensed, would enable legitimate individuals to be able to discharge such a burden of proof simply by indicating that they are licensed manufacturers.[307] The industry would accordingly operate in a

303 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

304 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003.

305 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

306 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

307 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002; Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 11 July 2003; Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003; Mr Jilluck Wong, Regional Director, Fraud Prevention, American Express, in conversation with the Committee, Sydney, 25 June 2003; Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003.

manner similar to that relating to the production of security paper for use in currency and cheques.

Among those the Committee spoke with, it was generally felt that an offence should be created of possession of any device or equipment that could be used in connection with the counterfeiting or production of plastic cards or commission of fraud in connection with payments systems, and that such an offence should be as technology-neutral as is possible in order to anticipate technological developments in the future.[308]

However, the Committee feels that the creation of harmonised laws throughout Australia (and indeed internationally) is the most desirable course to follow, as conduct of this nature is regularly perpetrated across jurisdictional borders. Accordingly, the Committee believes the most effective response is to refer the question of enacting appropriate uniform legislation to proscribe the manufacture, importation, possession and use of devices or other equipment that could be used to commit fraud in connection with payment systems to the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys General for investigation and report. The Committee was told that the Model Criminal Code Officers' Committee is already seeking to obtain such a reference from the Standing Committee of Attorneys-General.[309]

308 Commissioner Mal Hyde, South Australian Police, in conversation with the Committee, Adelaide, 3 October 2003; Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

309 Mr Matthew Goode, Managing Solicitor, Policy and Law Section, Attorney-General's Department, in conversation with the Committee, Adelaide, 3 October 2003.

Recommendations

44a. The Committee recommends that the development of a national legislative response to questions of theft of identity, identity-related fraud and credit card fraud including card skimming and the possession of equipment or devices used in connection with credit card fraud be referred to the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General for investigation and report. In doing so, consideration should be given to:

i. The introduction of an offence of assuming a false identity with the intention to commit a serious offence;

ii The introduction of offences proscribing the possession of equipment or devices (including plastic cards), with intent to dishonestly counterfeit or alter documents or to assist in the commission of an offence involving dishonesty;

iii. The introduction of offences proscribing the importation, possession and use of equipment or devices (including plastic cards), with intent to dishonestly obtain funds through the deception or manipulation of payment systems; and

iv Reversing the onus of proof.

44b. The Committee recommends that criminal offences relating to theft of identity, identity-related fraud or credit card fraud should not be implemented until a national approach to these issues has been agreed upon.

44c. The Committee recommends that any new criminal offences relating to theft of identity, identity-related fraud or credit card fraud should be technology-neutral.

Computer crime

In order to provide an effective legislative response to electronic commerce-related crimes, the Committee supports the harmonisation of computer crime offences in all Australian states and territories, and federally. The work of the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General has led to the enactment of legislation by the Australian government in 2001, the *Cybercrime Act 2001* (Cth), which was assented to on 1 October 2001 and commenced operation on 21 December 2001. This Act inserts a new Part 10.7 (Computer Offences) into the Commonwealth *Criminal Code Act 1995* (Cth) and thus provides model computer crime legislation for Australia.

The *Cybercrime Act 2001* (Cth) largely follows the provisions of the Council of Europe's *Convention on Cybercrime* and, although limited in its Commonwealth focus, the *Cybercrime Act* significantly improves the scope for prosecuting cyber criminals by introducing substantive offences and procedural provisions consistent with those of the Convention. This Convention 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. By December 2003, 33 of the 44 members of the Council, and all of the four non-member states involved in elaborating the document, had become signatories. However, Albania, Croatia, Estonia and Hungary were the only countries that had ratified the instrument, and five ratifications (three of them from member states) are required for the Convention to enter into force (Council of Europe 2001).

The new *Criminal Code Act 1995* offences follow certain parts of the Convention including the offence of 'unauthorised access, modification or impairment with intent to commit a serious offence' (s.477.1), which goes well beyond the *Computer Misuse Act 1990* (Eng) which was the original model. The *Criminal Code Act 1995* (Cth) 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 maximum penalty for failure to comply with such an order is six months' imprisonment (s.3LA *Crimes Act 1914* (Cth) and s.201A *Customs Act 1901* (Cth)).

Victoria has recently enacted comparable legislation, the *Crimes (Property Damage and Computer Offences) Act 2003* (Vic), which was assented to on 6 May 2003 and which has created a range of computer-based criminal offences based on the Commonwealth's *Cybercrime Act 2001* (Cth). New South Wales has also followed the Model legislation with the enactment of the *Crimes Amendment (Computer Offences) Act 2001* (see *Crimes Act 1900* (NSW) ss.308–308I), as has the Australian Capital Territory (*Criminal Code 2002*, ss.112–121, replacing provisions under the *Crimes Act 1900*). South Australia has recently introduced a Bill to amend its computer crime legislation along similar lines (Statutes Amendment (Computer Offences) Bill 2003 introduced in the House of Assembly 15 October 2003). The other jurisdictions are yet to amend their laws to follow the Model provisions.

It can be seen from the statistics provided in Appendix F that charges in relation to previous legislation continued to grow, although there have been relatively few matters recorded by Victoria Police under the new legislation. In 2002/03, for example, only 15 computer crime offences were recorded in Victoria (see Figure 3.5, Chapter 3). It remains to be seen how the introduction of this new legislation will affect the prosecution and outcomes of computer crime in Victoria.

Part of the reason for the relatively low number of recorded computer crime offences is that often crimes involving computers will be charged as ordinary property crimes. In September 2003, a 22-year-old man who encoded data from his mother's bank card on to a Time Zone Power Card and then re-configured a disused National Bank EFTPOS machine to imitate terminals of 19 businesses

in order to obtain 102 refunds worth $100,699, was charged with obtaining and attempting to obtain financial advantage by deception rather than computer crime offences. Judge Hogan sentenced him to two years and three months' imprisonment with a non-parole period of nine months (R. v *Weishaupti*, County Court of Victoria, 19 September 2003. See Lapthorne 2003).

Electronic commerce

The 52nd Parliament of Victoria's Law Reform Committee has observed:

> The main legal issues that arise in electronic commerce relate to identity and the security and privacy of electronically transmitted and stored information. These issues include how to:
>
> (a) ensure that a person who purports to electronically sign and/or lodge a document is in fact the person who signed and/or lodged the document;
>
> (b) ensure that the document sent by a person is received and stored in the same form in which it was sent;
>
> (c) prevent unauthorised access to documents during transmission and once stored (Parliament of Victoria, Law Reform Committee 1999, p.112).

Specific measures to address these concerns have recently been implemented in Victoria to facilitate the confidence of consumers in taking their business online. The *Electronic Transactions (Victoria) Act 2000* (Vic), came into operation on 1 September 2000 and is modelled on the *Electronic Transactions Act 1999* (Cth), which is based on UNCITRAL Model law on E-commerce of 1996.

The Victorian Act removes legal obstacles to conducting transactions by electronic means in Victoria. It gives effect to electronic signatures without committing to an exclusive definition of what those are, so as to allow contractual dealings such as offers, acceptances and invitations to be undertaken online. As the second reading speech makes clear, the legislation was drafted in line with the twin principles of functional equivalence (putting electronic means of contracting on the same legal footing as paper contracts) and technology neutrality (meaning that it is not restricted to any particular electronic technology, leaving room for future developments) (Parliamentary Debates, Victoria 2000a).

This intervention was intended to remove any uncertainty about whether transactions conducted entirely through electronic media could be supported by law. In our legal tradition, an ancient formal requirement governing a contract was the requirement of writing. It was enshrined in law as early as 1677, when the Statute of Frauds was enacted, with the aim of 'prevention of many fraudulent practices, which are commonly endeavoured to be upheld by perjury and subornation of perjury' (Khoury 1990, p.822). By specifying that agreements generally needed be written in order to be legally enforceable, those agreements would always be documented and hard evidence of them available.

This requirement has persisted over more than three centuries, but the rapid rise of information networks as an alternative means of communication to ink and paper has almost rendered it obsolete. The new Acts extend the application of the law of contract into cyberspace, with two important exemptions – in the area of wills and court documents. In these areas too the old rule is likely to give way eventually as technology moves ahead. This is enabling, as opposed to regulatory, legislation, so it does not in itself deal with the fraud (or other) risks accompanying electronic commerce.

Consumer protection

Also relevant in terms of state legislative responses is the area of consumer protection and fair trading. These laws require minimal adjustment to accommodate business activities conducted via the new technologies of electronic commerce, because the character of many of these offences is such that the technology used to mislead or deceive is irrelevant – an offence of this kind may be committed regardless of the medium. In Australia, the primary piece of consumer protection legislation is the *Trade Practices Act 1974* (Cth), but there is complementary fair trading legislation in each Australian state and territory. A simple example of a technology-neutral law against an unfair business practice is the prohibition of 'Pyramid selling' under that Act (ss.61 and 75AZO).

In Victoria, relevant provisions may be found in a number of different Acts. The *Goods Act 1958* (Vic) sets certain implied terms for contracts for sale of goods. In a sale of goods by a seller who sells the goods in the course of a business, there is an implied condition that the goods are of merchantable (reasonably good) quality and condition (ss.19(b) and 89). Where goods are sold by a description it is required that the goods in fact match the description (ss.18 and 87).

For a non-contract sales agreement, the *Fair Trading Act 1999* (Vic) stipulates in s.69(1) certain items of information that need to be given by the seller:

> (a) the total consideration to be paid or provided by the purchaser under the agreement;
>
> (b) any postal or delivery charges to be paid by the purchaser;
>
> (c) any rights the purchaser has under the agreement to cancel the agreement and how those rights may be exercised;
>
> (d) the full name of the supplier and either the full business address of the supplier or the telephone number of the supplier.

Under section 70, non-compliance may be penalised by a fine.

A further Victorian example is the *Introduction Agents Act 1997* (Vic), which was enacted to overcome unfair and unscrupulous practices in the introduction industry specifically. In section 4, 'introduction agent' is defined broadly as 'a person who carries on a business of providing, or offering to provide, an

introduction service'. Clearly the fact that a service may be provided online would not of itself exclude it from the ambit of the Act. The scheme set out in the Act includes registration of introduction agents (s.39) and restrictions on who may operate in the industry. For example, a person who had been convicted of a serious fraud offence within the previous five years would not be permitted to act as (s.14) or work for (s.18) an introduction agent. Basic requirements in relation to contracts and payments are given in Part 4. In addition, fines may be imposed for such practices as false advertising about the size of the client database (s.17) or misuse of the personal information provided by clients (s.19).

Finally, consider the wide applicability of the 'misleading or deceptive conduct' offence in section 52 of the *Trade Practices Act 1974* (Cth). The Australian Competition and Consumer Commission (ACCC), which enforces the Act, aims to promote competition and fair trading, and to provide for consumer protection. In late 1999 the ACCC reported that a corporation named 'The Australasian Institute Pty Ltd' had breached this section in the advertising, both print and online, for its Internet-based business courses. As a result of this finding the guilty party was required to offer refunds to certain students and display corrective advertising on its web site (Australian Competition and Consumer Commission 1999).

The company concerned in the above example was incorporated and based in Australia, which would have made it relatively easy to deal with in a fairly traditional manner. The real challenge presented by electronic commerce comes in policing and prosecuting cross-border frauds, particularly minor ones (see below). When it comes to Internet scams that take advantage of private consumers, prevention is far more effective than any cure. Unauthorised transfers of funds against financial institutions, whether perpetrated from inside or outside the organisation, require a very different response from frauds involving online scams against private consumers. Though both are fraud risks associated with electronic commerce, they require different – but concerted – responses. Any remotely effective solution in this area of consumer protection, for the foreseeable future, is likely to involve at least as much education and awareness-raising as active prosecution.

Information privacy

The issue of information privacy also overlaps with fraud or identity theft prevention. A sound legal basis for confidence in electronic commerce and information storage is an important part of the policy commitment to Victoria's place in the fast-developing information economy. And while information protection provisions may not appear to touch directly upon the issue of fraud in e-commerce, the efficacy of the legislative framework in this area will be a significant factor in determining the degree of vulnerability of personal information transferred over networks. With the amount of personal information held and dealt with electronically by public sector bodies, how

well the data protection principles translate into practice is a matter of crucial importance. Control of the growing risk of identity theft, and the many avenues of fraud leading from it, is essential in this area.

As the 52nd Parliament of Victoria's Law Reform Committee has noted, there is no general right of individual privacy at common law in Australia (1999, p.126). A greater recognition of privacy has long prevailed in certain situations, as in dealings between doctor and patient, or lawyer and client. However, statute has intervened in recent years in recognition of the importance of principled handling of personal information. The need for this reform was not simply a matter of defending people's sensibilities from the curiosity of impostors, but also a need in these times to guard against identity fraud and the tremendous damage it can cause.

The *Information Privacy Act 2000* (Vic), according to the second reading speech, was enacted as the second part of a package of legislation aimed at data privacy and security. (The first part was the *Electronic Transactions (Victoria) Act 2000*, discussed above.) The Act excludes from its ambit the health information of Victorians, which is covered instead by the *Health Records Act 2001* (Vic). These two Acts together provide the basis of information protection across the public sector in Victoria.

The Victorian information privacy legislation, which deals with handling of information in the public sector of the state, is intended to complement the Commonwealth *Privacy Act 1988*. The preamble to this Act indicates that it aims to meet Australia's responsibilities as a party to the International Covenant on Civil and Political Rights, and as a member of the OECD. It is clear that integrity, security and privacy of personal information are necessary to accord with internationally agreed principles of human rights, as well as from the more practical perspectives of crime prevention and law and order, which are the more predominant themes in this Report.

The Commonwealth *Privacy Act 1988* was amended in 2000 by the *Privacy Amendment (Private Sector) Act* and thereby expanded to cover the private sector across the country. This is important in view of recent overseas developments, notably the European *Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data*, which sets standards for information privacy across the European Union and stipulates that any other countries where personal information is to be sent must have equivalent protection in place. At the time of writing, only Argentina, Hungary, Switzerland, Canada and the United States were designated as having sufficient data protection legislation in place for EU members to safely send personal information there (European Commission 2003). It should be noted that there are alternative routes to enabling trans-border data flows; the fact that they do not yet appear on the list above does not prohibit EU businesses from engaging in electronic commerce with other countries. However, it has been questioned whether the Australian

approach is likely to meet the EU standard of data protection (see for example, Clarke 2000).

While the protection of information privacy can enhance fraud prevention by providing for the secure storage and transmission of personal data, some concerns have been raised that the scope of this legislation may also act to inhibit fraud control. In particular, it was argued that some of the provisions of the privacy Acts can prevent organisations from sharing information which may be useful for both preventing and detecting fraud.[310] While it was acknowledged that some of these concerns may be due to organisations misunderstanding the relevant legislation,[311] the Committee would be concerned if these Acts were providing an unjustifiable impediment to fraud control. However, the operation of both the *Information Privacy Act 2000* (Vic) and the *Privacy Act 1988* (Cth) both raise issues which extend far beyond the scope of the current Inquiry. The Committee therefore makes no recommendations in this area.

Spam

It was noted in Chapter 5 that certain types of fraud can be perpetrated by the sending of mass unsolicited email or 'spam'. The sending of such emails is considered to be a problem which is getting worse with time. It was suggested to the Committee that 'spam is a radically growing problem, [and] if it is not managed threatens to overwhelm the world's email system just at a time when the whole world is becoming dependent, for better or worse, on email'.[312]

The sending of spam raises a number of issues. Concerns have been raised about its privacy-invasive nature, the sending of pornographic material, and its general drain on computer resources. Of relevance to the current inquiry is the fact that these emails often contain fraudulent or deceptive material. The National Office for the Information Economy (2003) estimate that roughly half of all unsolicited bulk emails contain fraudulent information.

The sending of such information may already be regulated by consumer protection legislation, such as the *Trade Practices Act 1974* (Cth) and the *Fair Trading Act 1999* (Vic), which prohibit fraudulent or misleading conduct. In light of the increasing incidence of this problem, the Australian government has also recently taken specific regulatory steps. The *Spam Act 2003* (Cth), introduced with the *Spam (Consequential Amendments) Act 2003* (Cth), establishes a civil penalties regime regulating the sending of commercial electronic messages, including a prohibition on sending unsolicited

310 Mr Bruce Cox, Regional Director, Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003; Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

311 Acting Detective Superintendent Peter Lavender, Commercial Crime Division, Western Australia Police Service, in conversation with the Committee, Perth, 1 October 2003.

312 Mr Keith Besgrove, Chief General Manager, Regulation and Analysis Group, National Office for the Information Economy, in conversation with the Committee, 24 June 2003.

commercial electronic messages and regulation of general commercial electronic messages. Difficult questions have arisen, however, concerning the scope of the legislation and which agencies and organisations should be exempt from its provisions (Cant 2003). In view of the potentially large fines that could be imposed on offenders (up to $1.1 million a day for repeat organisational offenders), the Committee believes that further consultation is necessary.

While regulation of this area clearly raises issues beyond the scope of this Inquiry, the Committee supports initiatives designed to reduce the incidence of unsolicited email, which may be used to perpetrate fraud. Given the nature of this problem, the Committee believes that any response must be a national one.

Recommendation

45. The Committee supports national initiatives designed to reduce the incidence of unsolicited email ('spam').

Cross-border issues

Throughout this Report, the Committee has reiterated its belief that a national response is required if fraud is to be dealt with effectively. One of the main reasons for this belief is the fact that many fraudulent activities are committed across jurisdictions. This raises particular legal problems, as was noted by Mr Aub Chapman, Head of Operations at Westpac Banking Corporation: 'Laws that are passed in the state of Victoria are applied to the state of Victoria, but the trouble is the criminal doesn't stop at Wodonga. He moves over the border to Albury and continues…'[313]

This is a particular problem in the case of crimes committed electronically. In many cases of electronic fraud, suspects will never have set foot in the victim's country. Alternatively, while the offender may live in Victoria, the victim may be located in a different jurisdiction. Mr Alastair MacGibbon, Director of the Australian High Tech Crime Centre, described the cross-border problems associated with electronic crime investigation and prosecution:

> When one looks at any form of high tech criminality… jurisdictions are almost meaningless. Criminals may not even realise that they are crossing international jurisdictions when they are committing their crime. A hacker could be in Prahran and attacking someone in East Melbourne and not realise that they are actually bouncing through servers in a whole range of locations.

313 Mr Aub Chapman, Head of Operations, Westpac Banking Corporation, in conversation with the Committee, 24 June 2003.

> They may use a free email that is housed in a third jurisdiction; they may keep their hacking tools in a fourth.[314]

Where the offender and victim are not located in the same jurisdiction, there can be a problem in determining where the offence has occurred and therefore which law to apply, as well as a problem in obtaining evidence[315] and ensuring that the offender can be located and tried before a court. Additional problems can also occur in mobilising the law where offenders have fled the jurisdiction or moved assets overseas in order to evade confiscation.

The offence of stalking provides an example of these issues. Reforms currently before Parliament were partly motivated by the case of a Brighton man, Brian Sutcliffe, who was charged with stalking a Canadian television star with mail, telephone calls and emails, from 1993 to 1999. He was charged with stalking under the existing section 21A of the *Crimes Act 1958* (Vic), but the case was dismissed in the Melbourne Magistrates' Court because the victim, a Canadian resident, was held to be outside its jurisdiction (Robinson 2002). This decision was later overturned, but it highlighted the problem of the extra-territorial application of the offence.

Ideally, harmonising laws on a national and international basis would overcome such jurisdictional problems. If this were to occur, it would not matter where the offender and victim were located at the time of the offence. Unfortunately, such a solution is not likely to be implemented in the near future, if at all. In the meantime, one response is to make it clear that laws can still apply even if one party was not present in the state at the time of the offence.

This has been the response to the example provided above. On 19 November 2003, the *Crimes (Stalking) Bill 2003* (Vic) received its second reading in the Legislative Council. The proposed amendment, if passed, would cause the offence of stalking (including 'cyberstalking', by email and the like) to operate extra-territorially. If either the conduct alleged to constitute stalking or the victim of it were in Victoria at the relevant time, the Victorian offence could be charged.

The fraud-related offences in the *Criminal Code Act 1995* (Cth) have also been given extra-territorial application. For example, the offences contained in Divisions 134 and 135 (see above) have each been deemed to apply (a) whether or not the conduct constituting the alleged offence occurs in Australia; and (b) whether or not a result of the conduct constituting the alleged offence occurs in Australia. The Committee recommends the scope of all Victorian fraud and dishonesty-related offences be similarly defined. Such offences

314 Mr Alistair MacGibbon, Australian High Tech Crime Centre, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 24 October 2003.

315 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

should be able to be charged in any case where the offence was committed in Victoria, or where the victim was in Victoria.

It is important to note that the reform of legislation to create an applicable offence is only the first step toward resolving cross-border problems. If the case described above involved an offshore Internet user stalking a resident of Australia, the new legislation would enable a prosecution to take place, but if law enforcement agencies in the suspect's jurisdiction were unwilling or unable to assist in the arrest and extradition, little more could be done. The realities and limitations of international law enforcement at this time suggest that often minor trans-jurisdictional frauds will simply not be worth the resources required to investigate them. The cost-benefit analysis that makes co-operative effort a logical response to major organised crime, or terrorism, would not ordinarily apply to white-collar criminals acting alone.

In Australia, a package of measures was adopted in the late 1980s to facilitate the prosecution of organised crime and serious fraud. The first such measure was the *Mutual Assistance in Criminal Matters Act 1987* (Cth), which established mechanisms to facilitate international co-operation between investigators with respect to obtaining evidence; the location of witnesses and suspects; the execution of search and seizure warrants; the service of documents; the forfeiture of property and recovery of fines; and various other matters. The second was the *Proceeds of Crime Act 1987* (Cth), which enabled investigators to follow the trail of the illegal proceeds of crime internationally and to confiscate assets. The third measure was the *Cash Transactions Reports Act 1988* (Cth), which established a government agency to monitor the movement of large-scale cash transactions. Also adopted were the *Extradition Act 1988* (Cth), which extended Australia's ability to enter into extradition arrangements internationally, and the *Telecommunications (Interception) Amendment Act 1987* (Cth), which extended the ability of agencies to undertake electronic surveillance for law enforcement purposes. The International Branch of the Commonwealth Attorney-General's Department administers these pieces of legislation.

It is not difficult to imagine how the investigation of alleged crimes in diverse foreign jurisdictions may be both highly complex from a legal point of view and very costly. Procedures to allow inter-jurisdictional co-operation, including the facilitation by local authorities of foreign proceedings against Australian fraudsters, should be in place in order to secure the co-operation of other countries for investigations and prosecutions originating here. It is essential to realise that when it comes to cross-border criminal prosecution, as one commentator recently observed, good will and good intentions are not enough (Cassella 2002).

One area in which the Committee believes further research would be useful is the recovery of the proceeds of crime. In any international law enforcement operation the recovery of such proceeds is a complex question of intermeshing

separate and, to a greater or lesser extent, incompatible procedures and chains of authority. This has led to a perceived need to have legislation in place to act as an 'adapter', enabling local courts to freeze property at the request of a foreign state while forfeiture proceedings take place in their jurisdiction. Such a system is seen to be more efficient and reliable than a system based on professional courtesy alone, and removes confusion around the forum in which challenges to the forfeiture may be litigated (Cassella 2002). The Committee recommends that further investigations be undertaken to ascertain whether legislation should be passed giving Victorian courts this power.

It should be noted that the *United Nations Convention Against Transnational Organized Crime*, adopted unanimously by the General Assembly on 15 November 2000 (Resolution 55/25), offers some hope for future international harmonisation in the most serious instances of electronic fraud, where it is conducted in the context of organised crime. Among other things, its provisions seek to combat money laundering and corruption, and to facilitate international co-operation in expediting the seizure and confiscation of the proceeds of crime.

Recommendation

46. The Committee recommends that the issue of whether Victorian courts should be given the power to freeze property at the request of a foreign state while forfeiture proceedings take place in their jurisdiction be further investigated .

Procedural issues

Once a case of white-collar crime has been investigated it then remains for the evidence to be presented to the relevant prosecution agency. It is at this point that cases often founder, as prosecutors may believe that the evidence presented to them is inadequate or that the chances of success are insufficient to justify the time and expense involved in a lengthy trial. In cases involving electronic evidence it is sometimes only after the evidence has been presented to the prosecutor that evidentiary issues are detected. For example, the Committee heard that section 95 of Queensland's *Evidence Act 1977* requires computer records to be certified concerning their accuracy in order for evidence to be presented in court.[316] This can sometimes be an onerous procedure that can lead to critical evidence being excluded. A comparable provision in Victoria is to be found in section 55B of the *Evidence Act 1958* (Vic).

The prosecution of cases of serious fraud and non-compliance with the Corporations Law also requires the use of prosecutors with specialist training and experience. Recently some state and territory prosecution agencies disbanded specialist corporate prosecutions units, instead requiring such cases

316 Ms Leanne Joy Clare, Director of Public Prosecutions for Queensland, in conversation with the Committee, Brisbane, 26 June 2003.

to be dealt with by general prosecutions staff. This resulted in a loss of expertise that has impeded the investigation of complex corporate cases.

By contrast, the Commonwealth Director of Public Prosecutions continues to maintain a dedicated group responsible for corporate prosecutions. One of the fundamental tenets of justice is consistency in the manner in which offenders are handled. The heads of Commonwealth law enforcement agencies are currently taking steps to create overarching principles to ensure consistency between agencies in prosecuting serious and complex crime.

At present, where resources are severely limited, it is too often only the cases that attract considerable public attention or which involve substantial sums of money that are destined to proceed to trial. In order to demonstrate to the public that cases involving white-collar crime consistently receive appropriate attention by prosecutors, policies are needed which allow prosecutions to be mounted in as many cases as possible.

The Committee heard that although the prosecution of cases involving dishonesty sometimes raises complex questions, particularly if electronic evidence or cross-border issues are involved, the current prosecution policies used by prosecution agencies are sufficiently flexible to deal with such cases and probably do not need revision.[317] Of greater concern is the level of resources provided to prosecution agencies and the resulting difficulty in attracting the best individuals at a suitably attractive salary. It was observed that were it not for the fact that prosecution agencies attract the most interesting cases, even more prosecutors would probably leave for the private bar.[318]

One view expressed to the Committee was that policing and prosecution resources should be directed to particular kinds of matters. These matters were: those involving victims without the necessary resources or abilities to assist the police in the preliminary investigation of the matter; cases involving relatively small losses; and cases of organised criminal activity and money laundering. It was felt that the victims of major corporate fraud should assist in the investigation of matters of this nature.[319]

In 1992, the High Court of Australia in the case of *Dietrich* v *The Queen* ([1993] 67 ALJR 1) ruled that, unless exceptional circumstances exist, where a genuinely indigent accused person is unrepresented by counsel at a trial for a serious offence, the trial will be considered to be unfair and should be adjourned until legal representation is made available.

Few individuals are able to afford the costs associated with a long and complex criminal trial. Defendants charged with serious white-collar crimes are often

317 Ibid.

318 Mr Paul Coghlan QC, Director of Public Prosecutions, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

319 Submission from Mr Allen Bowles, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

able to arrange their financial circumstances in such a way as to make them appear indigent and thus able to take advantage of the *Dietrich* ruling. The effect may well be that a long and complex investigation is stayed indefinitely.

This situation has resulted in law enforcement agencies in some jurisdictions devoting considerable resources to certain serious fraud cases without any demonstrable result. Governments need to continue their efforts to counter this. The provision of legal aid may need to be extended and alternative strategies employed in order to reduce the costs of legal proceedings generally. In deciding how best to proceed, the effects of an alteration in the provision of legal representation need to be considered from the wider community perspective as well as taking into account the interests of those involved in the particular case.

A related issue concerns the prosecution of minors involved in electronic fraud and other computer crimes. As noted in Chapter 1, the nature of the technology is such that it is not only professional adults in the workplace but also self-taught teenagers at home who commit online 'white-collar crimes'. This presents certain difficulties for prosecutors. For instance, in 1993 an Edinburgh University student, Paul Bedworth, was tried under the English *Computer Misuse Act 1990* for computer hacking, some of which was engaged in when he was a minor. The offences with which he was charged involved access to various high-profile computer networks and systems including British Telecom, Lloyd's Bank and an EC computer system in Luxembourg. The jury acquitted him on the grounds of a purported clinical addiction to hacking, a defence which indicated that he had not formed the requisite criminal intent. His two co-accused, who were both several years older than he, pleaded guilty to certain offences and were sentenced to six months' imprisonment.

This case involved hacking engaged in for excitement rather than for personal gain. However, it suggests that in future cases courts may face a difficult challenge in striking the appropriate balance between, on the one hand, the need to deter people from engaging in damaging and expensive mischief online, and on the other hand, leniency towards young defendants who do not intend, or perhaps do not fully understand, the consequences of their actions.

Court processes

A number of inquiries into the criminal justice system have documented the problems associated with prosecuting white-collar crime. The first principal difficulty relates to presenting voluminous business and accounting records of complex financial transactions to a jury in such a way as to allow lay-people to understand the factual issues. The second difficulty is the length of time such trials take, which is often exacerbated in cases of criminal conspiracy by having multiple defendants and multiple charges. Each of these problems is said to exist in the Victorian criminal justice system concerning the prosecution and trial of fraud offences. Lengthy delays in having cases heard in the courts was said to be

a particular problem, with cases often taking a number of years to reach sentencing.[320] The submission of the Chairman of the Corporate Crime Liaison Group observed that 'there is a sense of resignation prevailing in the corporate community as to the criminal justice system's apparent inability to suppress the incidence of fraud and to deal with reported fraud in a timely and efficient manner.'[321] The factors contributing to this included: 'lack of resources generally, outdated and cumbersome legislation, lack of co-ordination across Australia at the legislative, executive and judiciary levels and an inability to keep pace with technological change.'[322]

Various reforms to court procedures were introduced throughout Australia during the 1990s to reduce the length, complexity and cost of prosecutions. Computer technology, for example, has greatly facilitated the presentation and analysis of complex business dealings. For example, in Perth the Committee conducted an inspection of an 'electronic courtroom' equipped with personal computers and projection facilities that enable the participants to view complex business records directly and to receive evidence from witnesses located in other countries. Although this courtroom, which cost $860,000 to establish, was created for the civil proceedings involving the Bell Group of companies, the facilities could just as easily be used in complex fraud prosecutions.

Some of the features of the court include 50-inch plasma screens, 17-inch LCD monitors, video players, DVD players, document cameras, video cameras and digital audio for court reporting, touch screen controls from the associate's desk and a master control that can be easily passed to counsel or the judge as the need arises. The Judge, counsel bench and associates all have personal computers, with the judge being on a separate network. To protect against viruses and unwanted data entering the network, three firewalls are present (Tarling 2003).

The Committee heard that the use of digital technologies in Victorian courts has increased considerably in recent years and although they are most often used in civil proceedings, there is great potential for computers to be of benefit in complex criminal trials as well.[323] Court administration in Victoria is also seeking to encourage more extensive use of electronic technologies in all aspects of legal proceedings (see Supreme Court of Victoria 2002).

In addition, legal practitioners are now closely regulated with respect to the length, manner and nature of material they present to the courts. The use of

320 Submission from Mr Geoff Griffiths to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 10 July 2002.

321 Submission from Mr Allen Bowles, Chairman, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

322 Ibid.

323 Hon. Justice Frank Vincent, Justice of the Supreme Court of Victoria, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 November 2003.

'directions hearings' in criminal trials seeks to ensure that criminal proceedings go ahead appropriately and promptly through interlocutory stages, while mechanisms are in place that aim at the early resolution of factual disputes. However, these reforms have not yet been rigorously evaluated and might not be achieving the intended results. It has been argued, for example, that unless defence counsel are provided with real incentives, they are unlikely to comply with such novel procedures (Sarre 1995, p.297).

The Committee also heard that in New Zealand the Serious Fraud Office must determine within six months whether a full investigation is necessary and must then close the case or proceed to prosecute 80 per cent of cases within 12 months. Despite being stringent, these targets have been achieved by an office that deals specifically with serious fraud matters.[324]

The Committee also heard the suggestion that in complex cases it may be preferable to have specially appointed judges and lists to deal with the matters. In the Netherlands, for example, so-called 'techno-courts' are used, in which the presiding judge is technically competent in the case he or she is hearing, such as cases involving electronic evidence.[325]

In view of the complexity of criminal trials concerning white-collar crime, it is necessary for all those involved to be thoroughly trained in carrying out their duties effectively. Witnesses, particularly forensic accountants, need to be trained in the presentation of complex financial 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 should be trained not only in the particular evidentiary and procedural rules that apply in such cases but also in liaising effectively with accountants and financial advisers, particularly when presenting lengthy and complex computer-based financial records. Just as a specialist Bar now exists for dealing with such cases, so a specialist sector of the judiciary may need to be cultivated in order to ensure that judges with appropriate experience and financial and information technology skills are available to hear these trials.

Finally, jurors and lay witnesses in these cases should be provided with information that will enable them to understand the latest court procedures. In Queensland, for example, so-called 'jury packs', which contain simple charts that set out to explain the case, are used in complex fraud cases. These are put together by a financial analyst with relevant experience who works for the Director of Public prosecutions in such cases, and gives evidence explaining the charts. This avoids the necessity of calling multiple witnesses from financial

324 Mr David Bradshaw, Director, Serious Fraud Office, New Zealand, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

325 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

institutions to give such evidence.[326] Victoria Police also regularly uses charts and visual material.[327]

Alternatively, as one submission to the Committee stated, complex cases could be tried by judge alone, or by a judge with a panel of specialist assessors. It was submitted that this would reduce the length and cost of fraud trials.[328] The idea of removing juries in serious fraud cases was supported by Victoria Police, which argued that because most fraud investigations are complex and lengthy it is unlikely that a juror with limited knowledge or expertise in fraud and electronic commerce would have sufficient comprehension of the issues in these types of trials to produce a fair decision. From the perspective of Victoria Police, a panel of specialist assessors and a trial judge was considered to be a better alternative to hear complex fraud and electronic cases than trial by judge and jury.[329] Similarly, Mr Newlan of the Corporate Crime Liaison Group noted: 'We look at the amount of time that is spent on jury trials and the complexity of cases that are put before juries and really question whether the juries are qualified to sit in judgment of the facts in those cases that go on for so long'.[330]

The Director of Public Prosecutions in Victoria did not support the idea of trial by judge alone, pointing out that the challenge in these complex cases is to make the information simple, and that if this is done juries are quite capable of understanding the evidence and determining whether the defendant acted dishonestly.[331] Similarly, Mr Justice Vincent generally favoured retention of trial by jury, but suggested to the Committee that some particularly complex parts of the judicial process could be dealt with by the judge, leaving the jury with the final decision-making power.[332]

One recent study comparing the decision-making processes employed in serious criminal cases by judges sitting alone with judge and juries concluded that similar processes are adopted by each. This makes the presumed benefits of trial by judge alone less profound than previously thought (Waye 2003).

326 Mr Phillip Bennett, Financial Analyst, Office of the Director of Public Prosecutions, in conversation with the Committee, Brisbane, 26 June 2003.

327 Superintendent Philip Masters, Divisional Head, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

328 Submission from Mr Allen Bowles, Chairman, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

329 Submission from Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 16 August 2002.

330 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

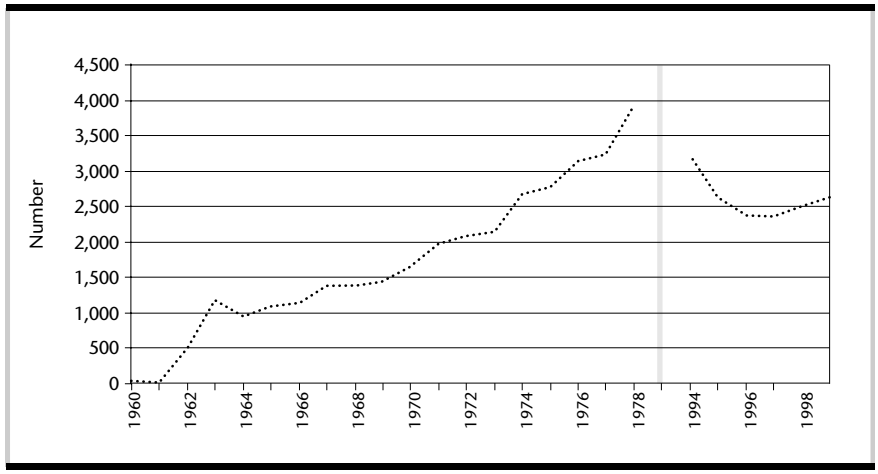
331 Mr Paul Coghlan QC, Director of Public Prosecutions, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

332 Hon. Justice Frank Vincent, Justice of the Supreme Court of Victoria, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 November 2003.

An indication of the workload of the criminal courts in cases involving fraud and deception can be found in official statistics reported in Victorian Yearbooks and in Sentencing Statistics, Higher Criminal Courts Victoria and Statistics of the Magistrates' Court of Victoria, published by the Victorian Department of Justice. Unfortunately there are some missing data in these series, and it must be emphasised that the categorisation of fraud and deception offences has changed over time. Counting rules for some statistical collections have also altered, making it difficult to present directly comparable time-series data in many cases. The Committee believes that the creation of the Victorian Fraud and Information Reporting Centre (VFIRC) as the central agency for the collection of information on fraud would greatly enhance the compilation of fraud statistics in Victoria.

For Magistrates' Courts, Figure 10.1 shows statistics of the number of fraud (as variously defined) convictions obtained between 1960 and 1979, and the number of principal proven fraud offences between 1994 and 1999. These are taken from separate series and are not directly comparable.

Figure 10.1: Victorian Magistrates' Courts, principal proven fraud offences, 1960–99



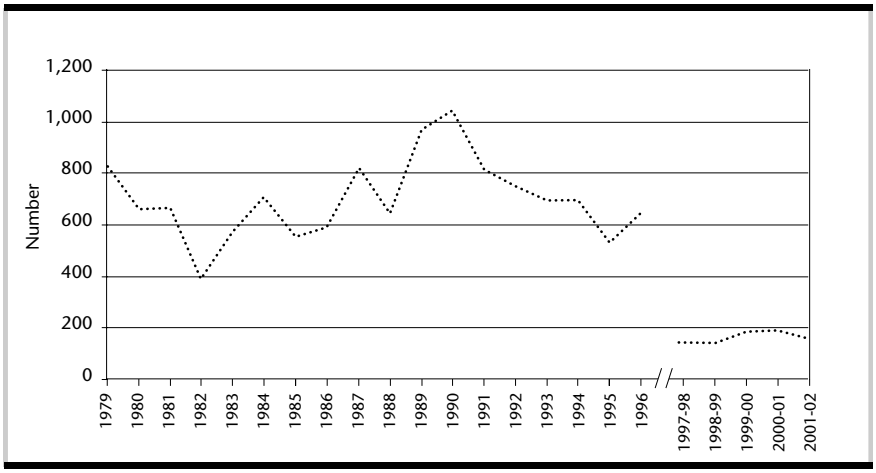
See: Notes to Appendix D for sources, raw data and definitions of offence categories used. Break indicates years for which statistics were unavailable.

For the higher courts (County Court and Supreme Court), Figures 10.2 and 10.3 show the number of sentences given for fraud offences (as variously defined) between 1960 and 2002 – these are shown in two separate figures to take account of the offence classification changes in 1978 which make the figures not directly comparable. In addition, following 1996, different counting rules applied for the higher courts statistics including a change to financial years rather than calendar years. These changes account for the smaller number of fraud offences dealt with since 1997/98. Details of the data presented in Figures 10.1 to 10.7 are contained in Appendix D.

Figure 10.2: Victorian higher courts, principal proven fraud offences, 1960–78

See: Notes to Appendix D for sources, raw data and definitions of offence categories used.

Figure 10.3: Victorian higher courts, principal proven fraud offences, 1979–2002



See: Notes to Appendix D for sources, raw data and definitions of categories used.

Recommendations

47. The Committee recommends that juries continue to be the appropriate body to make factual determinations in cases involving fraud and dishonesty-related offences. The Committee does not support the introduction of specialist juries, panels of assessors or trial by judge alone.

48. The Committee recommends that there should be specialist fraud lists in the Supreme and County Courts.

49. The Committee recommends that additional funding be allocated to the improvement of courtrooms in Victoria to enable information to be provided to judges, lawyers and members of juries electronically through the use of computers and displayed on screens in courtrooms during proceedings.

Sentencing

In Victoria, the following judicial punishments have been available in respect of fraud and dishonesty offences in recent years:

- fines;
- restitution and compensation orders;
- forfeiture and disqualification (confiscation);
- unsupervised release (suspended, deferred, conditional sentences);
- supervised release (probation, community service, intensive corrections); and
- custodial orders (either full-time or periodic) (Fox & Freiberg 1999).

There have been considerable changes in sentencing laws in Victoria, particularly since the 1970s, with various forms of supervised release becoming available. These developments are described comprehensively by Freiberg and Ross (1999).

Little research has been carried out in Australia on the manner in which white-collar offenders are dealt with following a criminal trial. In a study of a sample of 50 completed cases handled by the Major Fraud Group of the Victoria Police between January 1990 and October 1994, it was found that 68 per cent of offenders were sentenced to terms of imprisonment, usually less than five years; 14 per cent received good behaviour bonds; 11 per cent received suspended terms of imprisonment, 4 per cent were fined; and 3 per cent received community-based orders (Krambia-Kapardis 2001, p.100). However, these cases included some of the most serious fraud offences prosecuted in Victoria.

In the study of serious fraud cases in Australia and New Zealand undertaken by the Australian Institute of Criminology and PricewaterhouseCoopers (2003), 155 files were analysed. These related to 208 accused persons (165 males and 43 females), 183 of whom were convicted of offences. Of the sentences

imposed, full-time custodial sentences were given in respect of three-quarters of those sentenced. The mean maximum term of custodial sentences awarded was approximately 3.4 years, while the mean minimum custodial term awarded was almost 2.3 years. The longest custodial sentence was 11 years maximum with a non-parole period of eight years, awarded by the District Court of New South Wales following a trial of more than four weeks. The case involved the investment of over $10.3 million, a proportion of which had been fraudulently obtained from almost 300 victims.

Various forms of periodic detention, supervised release and unsupervised release were used in other cases but only three offenders received fines only and two offenders received compensation orders as the most serious sanction. In a number of cases, compensation or confiscation orders were made in addition to custodial terms. Males received proportionally more full-time custodial orders than females. Females, however, received higher proportions than males of supervised and unsupervised release orders. This does not necessarily reflect leniency toward female offenders in sentencing but rather is indicative of the nature of the offences committed, the amount of money involved and other aggravating and mitigating factors (Australian Institute of Criminology & PricewaterhouseCoopers 2003).

In determining sentence, courts not only take into consideration the factors raised by the offender in mitigation, but also a range of so-called aggravating factors. The top three aggravating factors mentioned by courts in sentencing were: a breach of trust, offending over a long period of time, and a large sum being involved. Male offenders tended to have a higher proportion of prior convictions than females, while females tended to have longer periods of criminality involved and repeated acts of criminality. Males also showed remorse less often than females and males tended to be less co-operative with the authorities than females (Australian Institute of Criminology & Pricewaterhouse Coopers 2003).

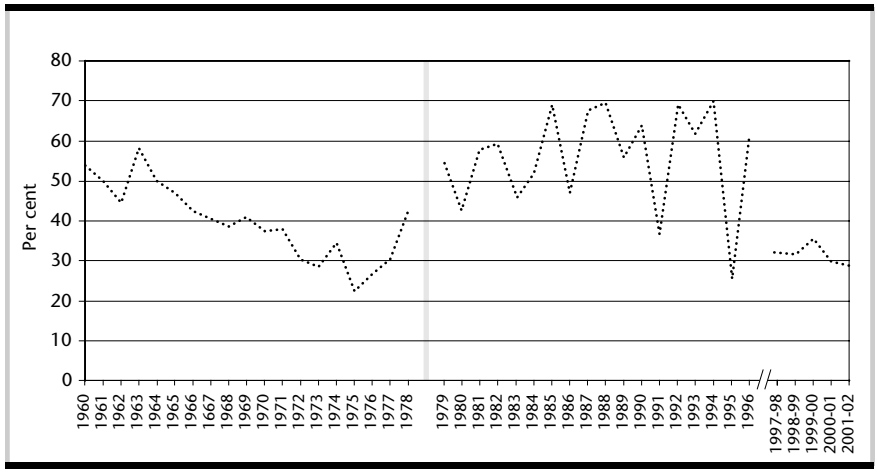
In an attempt to understand sentencing practices in Victoria, the Committee examined some statistics of sentences given in the higher courts from 1960 to 2001/02 in Victoria, and for Magistrates' Courts from 1997 to 1999 (see Appendix D for details). The Committee found, however, considerable difficulties with the statistical collections available, as some data were not collected or missing, while counting rules changed at various points in time making the presentation of consistent time-series data problematic. These problems need to be recalled when considering the following discussion.

It has been argued that white-collar offenders tend to receive non-custodial sentences more often than custodial sentences. The reasons given for this are that they are often first-time offenders; have co-operated with the police; have made financial restitution for their offences; may already have suffered other consequences of their wrongdoing, such as professional disqualification; and invariably they are proficiently represented by senior legal practitioners who are

able to describe their clients' mitigating circumstances in the most favourable light to the judge. Some have also been persons of high standing in the community.

Statistics related to this question have been calculated from official figures published between 1960 and 2002. Again, changes in counting rules in 1978 and 1997 make the data not directly comparable before and after these years. Figure 10.4 shows the percentage of custodial sentences given for the most serious offence involving fraud/deception out of the total number of sentences of all types given for the fraud/deception offences each year in Victoria.

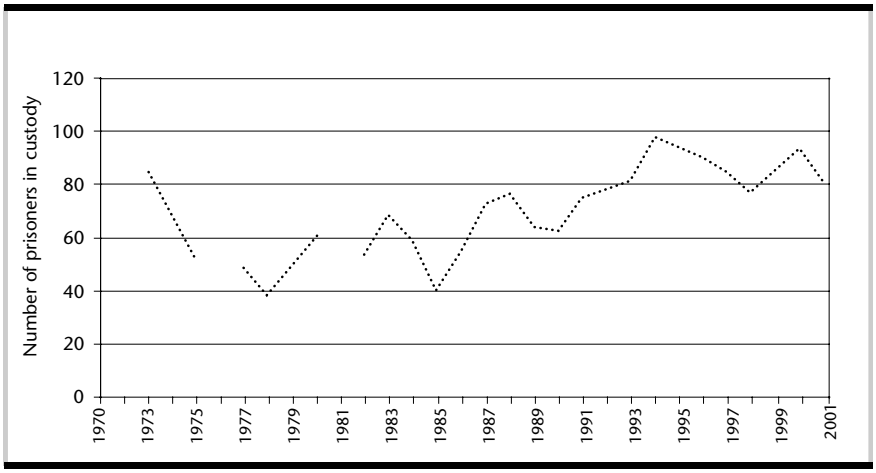
Figure 10.4: Percentage custodial out of total Victorian principal proven fraud offences in higher courts, 1960–2002



See: Notes to Appendix D for sources, raw data and definitions of offence categories used. Break indicates year in which statistics were unavailable.

Statistical information on the number of prisoners held in custody in Victoria for offences involving fraud and dishonesty (as variously defined over time) has been published by the Victorian agencies responsible for prisons for many years now. Since 1970, the number of prisoners in custody at 30 June each year whose most serious offence was fraud/deception have shown a general increase. The trends are shown in Figure 10.5, the raw data and the relevant category definitions for which are set out in Appendix D.

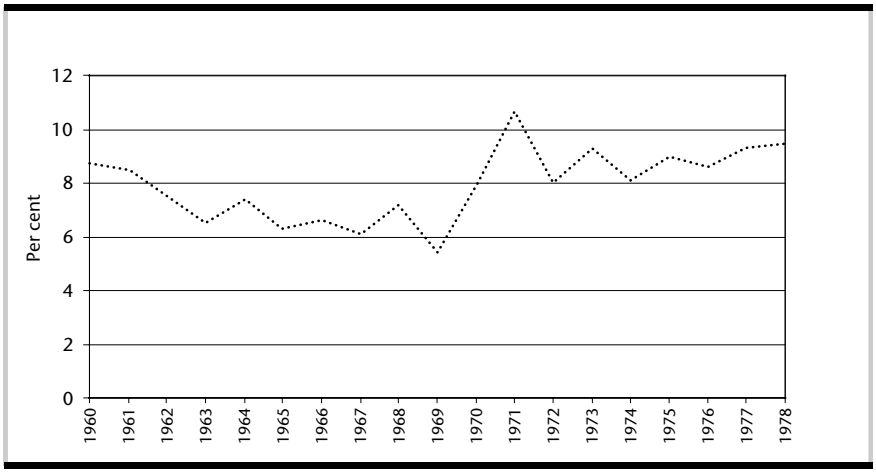
Figure 10.5: Victorian fraud prisoners in custody, 1970–2001



See: Notes to Appendix D for sources, raw data and definitions of offence categories used. Breaks indicate years in which statistics were unavailable.

As a proportion of the total prison population, prisoners whose most serious offence was fraud/deception have remained fairly constant, varying between 6 and 10 per cent of the total prison population between 1960 and 1978 (see Figure 10.6).

Figure 10.6: Percentage of prisoners' fraud offences out of total prisoners' offences, 1960–78

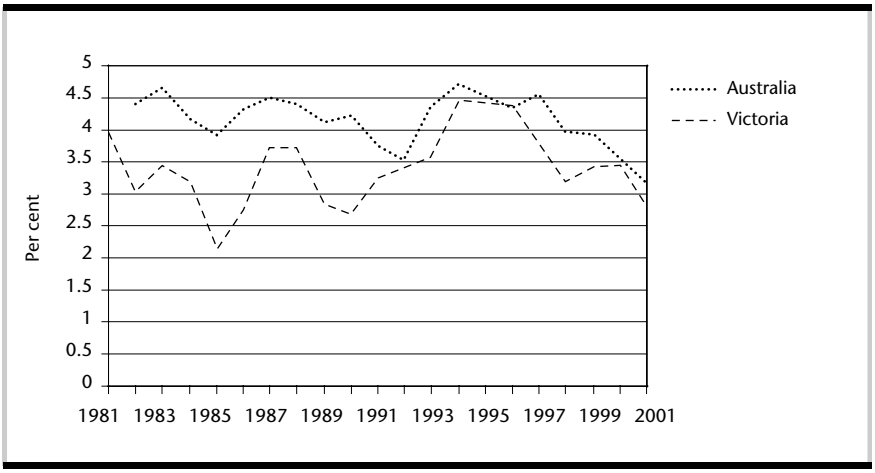


See: notes to Appendix D for sources, raw data and definitions of offence categories used.

Comparing the position in Victoria with the overall Australian prison population between 1981 and 2002, Figure 10.7 shows that there has generally been a lower percentage of prisoners in Victorian prisons serving sentences for most serious offence of fraud/deception than in Australian prisons overall (the following figure examines the percentage of prisoners whose most serious offence was fraud/dishonesty out of the total number of prisoners in custody at 30 June each year). In 2001–2002, for example, 2.47 per cent of the Australian

prison population was imprisoned for the most serious offence of fraud and misappropriation while in Victoria only 2.26 per cent of the Victorian prison population was imprisoned for the most serious offence of fraud and misappropriation. Over the last 10 years in Victoria, the percentage of the Victorian prison population imprisoned for the most serious offence of fraud and misappropriation has shown a continued decline and is now the lowest since 1960 (apart from 1985 when the percentage was 2.13 (see Appendix D)). Interestingly, in Victorian prisons on 31 December 1853 (the earliest year in which this statistic was recorded), 33 prisoners (3.46%) out of the total prison population of 955 were in custody with their most serious offence falling in the category 'forge, utter, fraud, embezzlement, obtaining goods under false pretences' (Inspector General of Penal Establishments 1855, Appendix B, p.17).

Figure 10.7: Percentage fraud offence prisoners out of total prisoners in custody, 1981–2001



See: notes to Appendix D for sources, raw data and definitions of offence categories used.

The extent to which severe sentences should be used for fraud offences has been subject to considerable debate over the years. It has been argued that sentences imposed on white-collar criminals have sometimes been inadequate:

> The sentences imposed on dishonest lawyers by the courts can be wildly inconsistent and sometimes, as in many cases of medical fraud, can seem pitifully inadequate compared with the sentences handed down on members of the public who steal similar amounts. When James Frederick pleaded guilty in the Supreme Court in Melbourne in 1978 to five counts of misusing trust money involving almost $50,000, he was only placed on a $50 good behaviour bond (Hall 1979, p.71).

The Committee heard that there was a perception that Australian sentences for fraud offences were lower than in other countries, thus making Australia an

apparently softer target.[333] On the other hand, doubts were expressed to the Committee as to whether severe sentencing had any real deterrent effects.[334] Sentences of substantial terms of imprisonment have been awarded in some instances (see Appendix D for details) and Detective Senior Sergeant Peter Wilkins of Victoria Police indicated that appropriately severe sentences were being imposed on serious fraud offenders in Victoria.[335]

Judicial punishments have been described as operating within an enforcement pyramid in which the most severe penalties, which are seldom used, sit at the top of the pyramid, while the least severe penalties, which are frequently used, fall near the base of the pyramid. Thus, non-judicial regulatory responses such as warnings appear at the base of the pyramid, in that they are used most often (see Ayres & Braithwaite 1992). It has been argued that compliance with laws can be maximised where a hierarchy of sanctions exists in which the most severe forms of punishment, such as incarceration, are available but seldom used. In the words of Ayres and Braithwaite, 'the more sanctions can be kept in the background, the more regulation can be transacted through moral suasion, the more effective regulation will be' (1992, p.19).

However, the perceived severity, as well as the effectiveness, of individual sanctions depends not only on their frequency of use but also on how they impact upon the individual circumstances of the offender. One submission received by the Committee expressed the view that the effect of a custodial sanction had greater impact on the offender's family than on the offender himself.[336] More imaginative sanctions than the conventional judicial penalties are available and should be considered even for serious white-collar offenders. These include adverse publicity, professional disciplinary sanctions, corporate probation, civil action, community service, injunctive orders and, most recently, various forms of reconciliation or community conferencing. These can all be used within the existing sanctioning structure, though they may require a little imagination from prosecutors and judges.

Braithwaite describes the utility of so-called 'equity fines' in which companies are ordered to issue a certain proportion of new shares, which are given to victims or to the state (1992, p.170).

333 Submission from Mr Glenn Bowles, Director – bRisk Australia Pty Ltd., to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 7 July 2003; Mr Bruce Cox, Regional Director, Global Security, American Express, in conversation with the Committee, Sydney, 25 June 2003.

334 Mr Dean Newlan, Corporate Crime Liaison Group, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 September 2003.

335 Detective Senior Sergeant Peter Wilkins, Major Fraud Investigation Division, Victoria Police, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

336 Submission from Ms G. Calabrese to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 July 2002.

The Committee also heard of the benefits that could accrue from the use of civil recovery proceedings taken in conjunction with criminal action.[337] Such proceedings differ from restitution in that they enable costs additional to the cost of the property stolen to be claimed, such as court costs, processing time, staff costs for arrest, and the cost of ongoing measures to prevent fraud. This is essentially a victim-led process in which the victim controls the timing and determines whether to pursue the offender. Clearly civil recovery would only be appropriate where an offender has assets and so some initial review of the offender's financial circumstances would be required. In the United States and the United Kingdom, the use of civil recovery action has apparently led to considerable reductions in property crime. In the opinion of the Committee, however, Victorian courts currently have adequate powers to impose financial sanctions, including compensation orders and restitution, and although their use could be made more extensive, additional legislative authority is not required at present.

Another example of how restorative justice approaches can work is seen in the case of Colonial Mutual Life Insurance agents who had fraudulently sold insurance policies to impoverished Aboriginal people in remote communities. During the settlement process, senior executives were forced to meet the victims of the scam and to live with them for a period in the Third World conditions in which they lived (Fisse & Braithwaite 1993, p.236).

The confiscation of an offender's assets represents an effective means of deterrence as long as such sanctions are widely publicised. In this sense, it is not so much the severity of the sanction but the probability with which it will be imposed that will enhance deterrence. Both adverse publicity and forms of reintegrative shaming can be effective in public sector workplaces where reputations are important. One form which has been found to be effective in reducing the extent to which staff use the Internet for unauthorised purposes involves employers publicising details of web sites visited by individual employees. Similarly, adverse publicity can have profound effects in terms of shaming an offender before the community, perhaps more so than the more common understanding of undertaking anonymous community service.

Disqualification as a company director may in some cases be a far more effective sanction to impose for dishonesty than a severe fine. The effect of sentencing on an offender's family and associates also needs to be considered. In one submission received by the Committee, the wife of an offender convicted of fraud described the serious consequences suffered by her and her family during the term of the offender's imprisonment. In addition, she highlighted the absence of effective rehabilitation offered to her husband during the period of his incarceration.

337 Mr Shane Ringin, General Manger, Pro Active Strategies Pty Ltd, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

In addition, instead of looking only to sanctions, it has been suggested that those who demonstrate high professional standards of conduct should be given praise and rewards that would help to foster an ethical professional culture (Sampford & Blencowe 2002). This idea is not new in discussions of compliance but could be used to positive effect in professional contexts (see Grabosky 1995).

Those who believe that judges are too lenient in sentencing white-collar offenders often seek to have maximum legislative penalties increased. Already, however, the maximum penalties which attach to serious white-collar crimes reflect the seriousness of such conduct, with lengthy terms of imprisonment and substantial fines being available. The extent to which long terms of imprisonment constitute a deterrent to white-collar crime is open to debate. While many property offenders behave more impulsively, white-collar offenders are relatively likely to engage in rational calculation, making some assessment of the prospective benefits and costs of a given fraudulent course of action. In these circumstances, the greater the perceived likelihood of conviction and the more severe the expected punishment, the less the inclination to offend. Individuals who are aware, for example, that their assets may be confiscated after a criminal conviction may consider that the benefits to be derived from offending are not worthwhile. The continued use of assets forfeiture legislation such as that which operates under the *Proceeds of Crime Act 1987* (Cth) and *Confiscation Act 1997* (Vic) is beneficial and deserves increased publicity.

Recommendation

50. The Committee recommends that maximum penalties for fraud and deception-related offences be consistent with those set out in the *Criminal Code Act 1995* (Cth).

Support services

One area in which the Committee received a number of submissions concerned the desirability of support services being provided for the victims of financial crimes. In addition to financial losses, which can be devastating, victims of fraud are also often seen as undeserving of support, perhaps owing to their perceived greed, stupidity for having been victimised by a confidence trickster, and occasionally for having brought the problem on themselves. Often these perceptions are incorrect, but those affected nonetheless suffer as a result.[338]

The argument was raised that the services provided by victim support agencies, which have traditionally focused on the victims of violent crime, need to be extended to the victims of economic and white-collar crime as well. One submission received by the Committee found traditional victim

338 Submission from Ms Patricia Farnell, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 August 2003.

support agencies of no help whatsoever in dealing with the victims of white-collar crimes.[339]

In particular, the Committee heard that specialist victim support services are needed for those who fall prey to identity fraud offenders, as often complex procedures are required to reinstate one's credit rating after it has been destroyed through the acts of an identity thief. Ideally, a central clearinghouse for complaints of fraud would enable support services and information to be provided efficiently from a single source. The Committee believes that the creation of VFIRC would solve this problem. Where a central agency gathers information of fraud victimisation, it would then be possible for the individual victim to refer other individuals and businesses to that agency to obtain verification that victimisation has indeed occurred and that the victim was not involved in the illegal conduct. The establishment of VFIRC would provide a central, authoritative agency within Victoria that could carry out this function on behalf of all victims of fraud and dishonesty in this state. In time, if an Australian Fraud Centre were established, this would help disseminate information throughout Australia.

Recommendations

51a. The Committee recommends that VFIRC be the central agency within Victoria responsible for co-ordinating support services for victims of fraud-related offences and their families, including victims of identity theft.

51b. The Committee recommends that procedures be developed to assist victims of identity theft to recover any loss or damage sustained as a result of the theft, including restoration of their credit rating. Consideration should be given to:

i. the development of a formal certificate (with appropriate security) outlining the name of the victim and the offence, which could be used to prove that they have been the victim of a crime; and

ii. the development of a standard affidavit for victims of identity crimes to be used by victims trying to counter the effects of identity theft, alleviating the need for filling out multiple forms.

51c. The Committee recommends that VFIRC provide information to victims of identity theft, including steps that can be taken to recover any loss or damage sustained as a result of the theft.

339 Submission from Ms G. Calabrese to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 July 2002.

Conclusion

Taking criminal action in the area of fraud and white-collar crime is neither simple nor quick. Financial considerations mean that only the most serious cases involving substantial monetary losses are likely to be investigated and tried, with the attendant possibility of convicted offenders receiving the most severe sanction of a term of imprisonment. The legal response to fraud control has, therefore, been severely restricted, although the possibility of criminal prosecution and sanction has always remained open.

Of course, the practical challenges of implementing legislative reform are many. One senior prosecutor from Northern Ireland recently observed in the context of computer crime that 'as with any legislation, it is not the passing of it that deters offenders, it is the success of its enforcement' (Bell 2002). Reforms are needed that will result in tangible outcomes.

A number of problems arise out of the current regulatory framework for dealing with fraud. First, there is a multiplicity of rules governing individual conduct that are to be found in civil and criminal laws, other regulatory statutes and codes of conduct which statutory professional bodies administer.

There is also a proliferation of ways in which individuals are regulated and a duplication of complaint-handling procedures. Fraud may be investigated by the civil and criminal courts, registration authorities and a variety of consumer-oriented statutory bodies such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, Departments of Fair Trading, Ombudsmen and Complaints Commissioners within certain professions.

Dishonest conduct therefore may be scrutinised from a range of perspectives that result in investigations being both time consuming and expensive to administer. Each system also has conflicting aims and overlapping sanctions. The Committee believes that its recommendations will assist in co-ordinating the legal response to fraud and white-collar crime in Victoria, which will, hopefully, reduce the incidence of crime of dishonesty, enhance deterrent effects and assist those who have been victimised through dishonest practices.

11. Conclusion: Key Issues for the Future

Introduction

This Report has sought to provide as much information as is currently available on the nature and extent of fraud in Victoria and the likely fraud risks that will affect the use of electronic commerce in the future. Other states and territories, the Commonwealth and other countries are equally affected by fraud and although the Report has primary relevance to Victoria, hopefully the solutions that have been canvassed here may be relevant to and co-ordinated with those in other places.

This final chapter summarises some of the key areas discussed as well as the primary directions for future research.

Integrated response

The ease with which fraud transcends domestic and international jurisdictional boundaries, especially in the electronic commerce context, necessitates a high degree of co-operation between law enforcement and regulatory agencies. Fraudulent schemes may be launched in new markets where potential victims are unwitting and highly vulnerable. It is therefore highly desirable that information about current and emerging manifestations of dishonest conduct be shared widely among law enforcement and regulatory agencies so that appropriate action may be taken as soon as possible.

National approaches such as that adopted by the Australian Crime Commission and the Australian High Tech Crime Centre are important in responding effectively to cybercrime and fraud that takes place across jurisdictional boundaries. So too are national professional organisations such as the Australian Nursing Council Inc. and the Law Society of Australia, as well as private sector business ventures such as the Australian Institute of Professional Investigators, which was established by a number of firms of accountants and consultants.

In addition, co-ordination is necessary between Commonwealth and state and territory agencies involved in issuing documents used to establish identity. Sharing of information is one of the most effective ways of preventing offenders

from abusing the 100-Point system, although any data sharing needs to be carried out with due regard for privacy requirements.

Policing white-collar crime is becoming more complex and therefore requires collaboration with business and technological specialists. There is an increasing need to integrate public and private sector crime prevention and investigation endeavours. For instance, those with forensic accounting and legal skills will perhaps be retained to assist police in certain technical investigatory functions. Specialist training in fraud investigation should be conducted as widely as possible both within and across agencies and, where possible, training programs should employ uniform approaches to enable personnel to move freely between agencies as required. Consultants with expertise in particular types of investigations could also be used to supplement existing staff. Agencies throughout the public and private sectors, particularly those engaged in criminal justice administration, need to continue contributing resources to the creation and maintenance of specialist units that have particular expertise in dealing in complex commercial crime.

Sources of information

Before the problem of fraud and white-collar crime in Victoria can effectively be addressed, much more extensive information needs to be gathered on the nature and extent of the problem and how it is handled. The desirability of enhancing the quality of statistics in this area is, however, matched only by the difficulty of achieving this goal. Given the wide range of activities categorised as dishonest, and the proliferation of public and private institutions involved in controlling the problem, it would be naive to aspire to perfect knowledge. However, it is important to strive towards a greater degree of uniformity across regulatory agencies and between state, territory and Commonwealth agencies in recording and reporting practices.

In addition, there is a need for victims of fraud and white-collar crime to be persuaded to report their victimisation, for strategic and statistical purposes as well as to take action against the perpetrators. Improved reporting requires effective procedures to be in place to protect confidential business information and to assure victims that the processes of reporting and prosecution will be cost-effective and sensitive to their interests.

In particular, there is a need for individuals who report crime in the public interest to be protected from discrimination and reprisals. Legislative protection now exists in many jurisdictions throughout Australia, but its existence should be widely publicised and the relevant provisions used. Legal protection against proceedings in defamation and other civil legal action should also be in place and guarantees of anonymity and confidentiality should be available in appropriate circumstances for individuals who report matters to the authorities.

In certain cases where individuals acted in the public interest by reporting crimes of dishonesty and have suffered financially, compensation or other support may also be appropriate.

Education

There is also a need to enhance potential victims' knowledge of dishonest criminal activities, particularly those at greatest risk such as young people who may use new technologies and give insufficient consideration to the risks of fraud, and some older persons who may be targeted as potentially susceptible victims. Law enforcement agencies are well placed to share certain limited kinds of information with private citizens, businesses, and public sector agencies, a point stressed in the submission from the Corporate Crime Liaison Group to the Committee.[340] All prospective victims of crimes of dishonesty should be made aware of the types of activities to which they are most vulnerable, the most appropriate means of prevention, and the best avenues of response when they detect an offence.

The development of comprehensive codes of conduct, such as those implemented in the field of electronic banking, will not only provide a statement of benchmarked standards for those using such systems, but will also be useful in resolving disputes between individuals. Recently, for example, an Electronic Commerce Code of Conduct has been developed, entitled *Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business* (Department of Treasury, Consumer Affairs Division 2000). Some potential offenders would be deterred if they were made aware of the regulatory controls that are in place.

New developments in communications allow both the wide dissemination of basic information on the prevention and control of white-collar criminal activities and the immediate reporting of suspicious activities to appropriate authorities. The Internet abounds with materials on fraud prevention as well as sites maintained by regulatory agencies that give advice on how to lodge complaints. In addition, the Internet is now being used to publicise information about successful prosecutions, such as lists of banned financial advisers and deregistered doctors and lawyers. This reinforces the rationale for which many regulatory controls were originally established, that is to provide information to members of the public to enable them to identify legitimate and trustworthy professionals with whom they can transact business with confidence.

Most regulatory agencies throughout the world provide information in paper form and electronically through web sites that alert consumers to misleading and deceptive practices – the Consumer World web site has over 1,400 links to consumer protection and regulatory agencies (http://www.consumerworld.org).

340 Submission from Mr Allen Bowles, Chairman, Corporate Crime Liaison Group, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 30 August 2002.

The Australian Competition and Consumer Commission's web site also gives advice on pyramid selling schemes, business opportunity schemes, and fraudulent prizes and lotteries (Australian Competition and Consumer Commission 2001). Examples of recent and prevalent deceptive practices are listed along with the legal penalties that apply. In addition, and in order to enhance consumer confidence in the Internet, the Australian Government's Department of Communication, Information Technology and the Arts has produced a series of fact sheets that provide information to consumers about the risks of shopping online and other issues such as paying tax and duty, and privacy issues (Department of Communications, Information Technology and the Arts 1999). Similar advice is available in Britain at the Office of Fair Trading (http://www.oft.gov.uk) and in the United States at the Federal Trade Commission (http://www.ftc.gov).

Consumer interest groups also provide a good source of trusted information for consumers. Bodies such as the Australian Consumers' Association, the Consumers' Union of the United States and the Great Britain Consumers' Association conduct their own testing of products and services and publicise the results through subscriber-based magazines such as *Choice* (Australia), *Which* (United Kingdom) and *Consumer Reports* (United States).

Although consumer organisations already provide consumer information by various means, including the Internet, perhaps the role of these groups in providing information services could be increased.

Using technology appropriately

There is also a rapidly expanding industry that provides electronic security measures associated with electronic commerce. Some products are clearly better suited to the fraud risks of electronic commerce than others, and one challenge lies in choosing appropriate measures tailored to suit individual needs. However, the nature of this market is such that there are likely to be numerous approaches to the problems associated with electronic commerce, and effective solutions will comprise a combination of complementary approaches. It remains to be seen which of these will prove most effective in regulating the global market of the future. In the short term, businesses and government agencies should become aware of and evaluate products available, avoiding those that are inappropriate, unreliable, overly expensive or unsuited to their needs.

Changing attitudes

Most importantly, the effective prevention of fraud entails the development of a culture of intolerance to conduct of this nature throughout the community. Deceptive and manipulative practices, in whatever walk of life, should not be condoned. Recent lengthy sentences imposed on convicted perpetrators of commercial and professional crimes might help to convey this message. On 13 March 2003, for example, an accountant and former mayor of Geelong, Victoria

was sentenced to 10 years' imprisonment with a non-parole period of seven years after pleading guilty to defrauding his clients of $8.6 million between 1994 and 2000. He was known and trusted by many members of the Geelong community but abused that trust by stealing funds from a number of his clients. In one case, $4.98 million was stolen from a trust account established to administer an award of $6 million damages paid to the victim of medical negligence that had rendered him quadriplegic. After becoming one of the signatories to the bank account established to hold the client's funds, the offender made a number of unauthorised withdrawals that were used initially to replace sums stolen from other clients and subsequently for gambling (R. v *De Stefano*, [2003] VSC 68, Supreme Court of Victoria, 13 March 2003).

In addition, constructive education campaigns such as those used to help change attitudes about discriminatory practices in the community could be employed throughout Victoria, and indeed Australia, to explain why dishonest and corrupt practices are unacceptable. Perhaps substantial resources need to be allocated for achieving generalised changes of attitudes, from both public and private sectors. Compelling evidence exists to indicate that expenditure on such initiatives would be cost-effective in reducing losses sustained through white-collar crime.

For Victoria to compete in the global economy it must seek to maintain a reputation of high integrity. The Corruption Perception Index compiled by Transparency International, the Berlin-based Coalition Against Corruption in International Business Transactions, currently ranks Australia as eleventh lowest out of 102 countries in terms of the extent to which corruption is perceived to have an impact on commercial and social life. Australia was recently given a score of 8.6, with a score of 10 representing no corruption and 0 representing extreme corruption (Transparency International 2002). The national score and ranking have remained stable since the first survey in 1995. In order for Australia to maintain this level of business integrity it must deal effectively with instances of white-collar crime as soon as they emerge, and publicise the outcomes of successful legal proceedings.

In a number of submissions to the Committee, the point was made that the creation and maintenance of an ethical culture in business and government is the best way in which to reduce fraud risks. The Auditor-General of Victoria, for example, observed that 'the setting of an example from the top is critical if agencies are to successfully instil a culture of ethical behaviour and engender trust and commitment from staff in the corporate attitude to fraud'.[341] He also stated that:

> The placing of a high priority on ethical behaviour and living out that priority in practice would be great starting points in both the public and private sectors for

341 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003. See also the similar observations made by Mr Dennis Challinger, Consultant Criminologist, RLP Consulting, Evidence given at the Public Hearing of the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 4 September 2003.

> influencing public attitudes to offences of dishonesty. In other words, making transparent a commitment to high ethics and demonstrating the impact of that commitment over time would seem to be key strategic actions.
>
> In the public sector, leadership on ethics should feature prominently in the Government's direction and guidance to agencies and be conspicuous in agencies' corporate plans. These strategies should be backed up by transparent public reporting on the public sector's overall performance in reducing the incidence of fraud and achieving increasing levels of ethical behaviour.
>
> The ultimate aim, in terms of influencing public attitudes, should be to present the public sector's approach to managing and reporting on fraud, with its strong emphasis on transparency and accountability, as a model that should be emulated by the private sector.[342]

In the case of white-collar offenders who carry out their activities on the basis of some rational calculation, deterrence also remains an important component of fraud control. The confiscation of assets, in particular, represents one means of achieving deterrence in the case of economic crime, but this will be achieved only if offences are reported to the authorities and the outcome of proceedings widely publicised. The Committee heard that fraud is always going to be a risk of modern life, and that as technology continues to develop, particularly with respect to online commercial activities, increasingly large amounts will be misappropriated from individuals and organisations. The consequence is that such losses will inevitably be passed on to consumers. If fraud can be controlled it is likely that the community will benefit in two ways – first, through reduced direct losses, and secondly through a reduction in the cost of goods and services. The benefits are, therefore, likely to be considerable.

Although fraud and white-collar crime are often perpetrated using complex strategies to trick unsuspecting individuals into parting with money, and even more complex means to disguise the proceeds of dishonest activities, some of the most effective means of preventing such activities are often relatively simple and within the reach of everyone. The Committee believes that the information derived from its extensive inquiry into fraud and electronic commerce will provide a sound basis for enabling all Victorians and all Victorian organisations to understand the fraud risks which they face and how best to guard against them.

Adopted by the Drugs and Crime Prevention Committee
Level 8
35 Spring St
Melbourne

15 December 2003

342 Submission from Mr Wayne Cameron, Victorian Auditor-General, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 October 2003.

Appendices

Appendix A-1: List of Submissions

Submission Number	Name of Individual/Organisation	Date Received
1	Ms G. Calabrese	6 July 2002
2	Mr Geoff Griffiths	10 July 2002
3	Mr J.W. Cameron, Auditor-General, Victoria	14 August 2002
4	Mr Phil Clark	15 August 2002
5	Mr Neil J. Jensen, Acting Director, Austrac (Australian Transaction Reports and Analysis Centre)	16 August 2002
6	Commander Paul Hornbuckle, Corporate Policy & Executive Support, Victoria Police	16 August 2002
7	Confidential submission	21 August 2002
8	Mr Allen Bowles, Chairman, Corporate Crime Liaison Group	30 August 2002
9	Confidential submission	30 May 2003
10	Confidential submission	30 June 2003
11	Mr J.W. Cameron, Auditor-General, Victoria	3 July 2003
12	Mr Glenn Bowles, Director, bRisk Australia Pty Ltd.	7 July 2003
13	Ms Anne Tibaldi, Director, Organisational Development Department, Victoria Police	11 July 2003
14	Ms Patricia Farnell	4 August 2003
15	Mr Robert Antich, General Manager, Compliance Strategies, Australian Competition & Consumer Commission	3 October 2003
16	Mr J.W. Cameron, Auditor-General, Victoria	6 October 2003

Appendix A-2: Conferences and Seminars attended by Committee Members and/or Consultants

Serious Fraud in Australia and New Zealand, 1 April 2003, seminar organised by the Australian Institute of Criminology and PricewaterhouseCoopers, held in Melbourne.

Crime in the Digital Economy, 15 May 2003, seminar organised by Monash Law School and Clayton Utz, held in Melbourne.

Regulating in the Digital Economy, 15 July 2003, seminar organised by Monash Law School and Clayton Utz, held in Melbourne.

Financial Crimes Summit 2003, 28–30 May 2003, international conference organised by the International Association of Financial Crimes Investigators (IAFCI) and the Institute for International Research (IIR), held in Sydney.

Introduction to a Privacy Code of Conduct, 6 August 2003, seminar organised by the Biometrics Institute, held in Melbourne.

National conference of Parliamentary Oversight Committees of Anti-Corruption/Crime Bodies, 30 September–1 October 2003, organised by the Joint Committee on the Anti-Corruption Commission, Parliament of Western Australia.

Appendix B-1: List of Interstate Meetings and Site Visits

Canberra – 23 and 24 June 2003

Name	Position	Organisation
Mr Chris Clark	Acting Director	Australian Crime Commission
Ms Lisa Carr	National Fraud Desk and Identity Fraud	Australian Crime Commission
Mr Nigel Phair	Federal Agent	Australian Federal Police
Mr Nicholas Klein	Team Leader, High Tech Crime Team	Australian Federal Police
Dr Clive Summerfield	Manager for Government Services	VeCommerce Ltd
Mr Neil Mann	Deputy Commissioner	Australian Taxation Office
Mr Chris Barlow	Assistant Commissioner	Australian Taxation Office
Mr Rory Mulligan	Assistant Commissioner	Australian Taxation Office
Mr Greg Dart	Assistant Commissioner	Australian Taxation Office
Mr Peter Zdjelar	Director, Fraud Prevention and Control	Australian Taxation Office
Mr Keith Besgrove	Chief General Manager, Regulation and Analysis Group	National Office for Information Economy
Mr Phil Malone	E-Business Branch	National Office for Information Economy

Sydney – 25 June 2003

Name	Position	Organisation
Mr Aub Chapman	Head of Operations	Westpac Banking Corporation
Mr Mark Bezzina	Director, Communications, IT and eCommerce	Standards Australia
Mr Tom Godfrey	Director, Corporate and Public Affairs	Standards Australia
Mr Graham Austin	Manager, Fraud Minimisation	NSW Registry of Births Deaths and Marriages
Mr Tom Jambrich	Assistant Auditor-General	NSW Audit Office
Mr Stephen Horne	Director, Performance Audit	NSW Audit Office
Mr Jilluck Wong	Regional Director, Fraud Prevention	American Express
Mr Bruce Cox	Regional Director, Corporate Security, Asia Pacific Region	American Express
Mr Michael Outram	Executive Director, Strategic Operations	NSW Independent Commission Against Corruption
Mr Ted Dunstone	Previous Director	Biometrics Institute
Ms Louise Collins	Consultant	SAGEM
Mr Tony Vaccarella	Identification System Account Executive	SAGEM

Brisbane – 26 June 2003

Name	Position	Organisation
Ms Leanne Joy Clare	Director of Public Prosecutions	Office of the Director of Public Prosecutions
Mr Phillip Bennett	Financial Analyst	Office of the Director of Public Prosecutions
Mr Brendan Butler	Chairperson	Crime and Misconduct Commission, Queensland
Mr Ray Bange	Acting Manager, Misconduct Prevention Unit	Crime and Misconduct Commission, Queensland
Mr Tony Clowes	Officer in Charge, Forensic Computing,	Crime and Misconduct Commission, Queensland
Ms Narelle George	Officer Misconduct Prevention	Crime and Misconduct Commission, Queensland
Mr David Goody	Principal Financial Investigator	Crime and Misconduct Commission, Queensland
Ms Julianne Webster	Research Officer, Strategic Research Unit	Crime and Misconduct Commission, Queensland

Perth – 1 October 2003

Name	Position	Organisation
Commissioner Barry Matthews	Commissioner of Police	Western Australia Police Service
Acting Detective Superintendent Peter Lavender	Commercial Crime Division	Western Australia Police Service
Senior Constable Phillip Russo	Commercial Crime Division	Western Australia Police Service
Mr Stephen Kay	Director Business Improvement, Court Services Directorate	Supreme Court of Western Australia
Mr Shaun Major	Manager Business Services	Supreme Court of Western Australia
Mr Vageli Mitakos	UnisysWest IT Manager, Courts	Supreme Court of Western Australia

Adelaide – 3 October 2003

Name	Position	Organisation
Commissioner Mal Hyde	Commissioner of Police	South Australia Police
Mr Matthew Goode	Managing Solicitor, Policy and Law Section	Attorney-General's Department, South Australia
Mr Des Berwick	Executive Officer	Australasian Centre for Policing Research, South Australia

Appendix B-2: List of Meetings and Public Hearings in Melbourne

Witnesses Appearing at Briefings – 6 August 2002

Name	Position	Organisation
Andrew Tuohy	Senior Manager	KPMG Forensic

Witnesses Appearing at Briefings – 2 June 2003

Name	Position	Organisation
Detective Senior Sergeant Peter Wilkins	Major Fraud Investigation Division	Victoria Police

Witnesses Appearing at Public Hearings – 4 September 2003

Name	Position	Organisation
Mr Shane Ringin	General Manger	Pro Active Strategies Pty Ltd
Ms Liz Atkins	Deputy Director	Australian Transaction Reports and Analysis Centre (AUSTRAC)
Mr Andrew Tuohy	Senior Manager	KPMG Forensic
Mr Dennis Challinger	Consultant Criminologist	RLP Consulting
Superintendent Philip Masters	Officer-in-Charge, Major Fraud Investigation Division	Victoria Police
Detective Senior Sergeant Peter Wilkins	Major Fraud Investigation Division	Victoria Police
Superintendent Paul Ditchburn	Organisational Development Department	Victoria Police
Inspector Stephen Leane	Manager, Legislative Review & Proposals	Victoria Police
Ms Alison Creighton	Legal Project Officer, Legal and Corporate Policy	Victoria Police

Witnesses Appearing at Public Hearings – 15 September 2003

Name	Position	Organisation
Mr David Bradshaw	Director	Serious Fraud Office, NZ
Mr Dean Newlan	Secretary	Corporate Crime Liaison Group
Mr Tim Farrelly	Independent Researcher	-
Mr Paul Coghlan, Q.C.	Director of Public Prosecutions	Office of Public Prosecutions Victoria

Witnesses Appearing at Public Hearing – 6 October 2003

Name	Position	Organisation
Mr Edward Hay	Deputy Auditor-General	Victorian Auditor-General's Office
Mr Joe Manders	Assistant Auditor-General, Corporate Planning and Parliamentary Liaison	Victorian Auditor-General's Office
Mr David Reid	General Manager, Financial Audit	Victorian Auditor-General's Office

Witnesses Appearing at Public Hearing – 24 October 2003

Mr Alastair MacGibbon	Director, Australian High-Tech Crime Centre	Australian Federal Police
Mr Nigel Phair	Federal Agent, Australian High-Tech Crime Centre	Australian Federal Police

Witnesses Appearing at Public Hearing – 7 November 2003

Name	Position	Organisation
Hon. Justice Frank Vincent	Justice	Court of Appeal, Supreme Court of Victoria

Appendix C-1: Deception Offence Descriptions Recorded in Victoria Police Statistics

Category of Deception Offence (137 offence descriptions)	Listed Offence Description
Forgery (22 offence descriptions)	• Falsely apply trade mark to goods • Falsify an Australian passport • Make false document (Crimes Act) • Make instrument – forging reg trade mark • Possess goods for sale – forged trade mark • Possessing instrument for forging trade mark • Forge Commonwealth document • Forge/utter Commonwealth signature • Forge/falsify certificate • Forge/falsify other document • Possess goods for manufacture false trade mark • Possess goods for sale with false trade mark • Forge document deliverable to Commonwealth • Apply false registered trade mark • Sell goods – falsely apply reg trade mark • Make counterfeit money • Possess counterfeit money • Forge prescription – restricted substance • Forge prescription – drug of dependence • Fraudulently alter prescription • Alter prescription – drug of dependence • Forge licence / learner's permit
False documents (13 offence descriptions)	• Fail to keep records • Make copy of false document • Fraudulently alter registration label • Fraudulently alter document • Fraudulently use reg label/plate • Fradulently use document • Produce/use account to mislead/deceive321M • Produce/use account to mislead/deceive 321MG • Have custody false document (Crimes Act) • Make possess for another – false document • Make possess article to make false document • Falsify book – Commonwealth • Possess passport issued to another

cont…

Category of Deception Offence (137 offence descriptions)	Listed Offence Description
Cheque fraud (3 offence descriptions)	• Obtain advantage by valueless cheque • Obtain benefit by valueless cheque • Obtain credit by valueless cheque
Uttering / using false documents (16 offence descriptions)	• Uttering (common law) • Utter document deliverable to Commonwealth • Utter forged cheque • Expose goods for sale – forged trade mark • Sell goods – forged trade mark • Use false document (Crimes Act) • Use copy of false document (Crimes Act) • Uttering document issuable to Commonwealth • Utter counterfeit money • Utter counterfeit security • Buy/sell/receive/dispose counterfeit money • Utter altered script – restricted substance • Utter forged script – restricted substance • Utter forged script – drug of dependence • Utter altered script – drug of dependence • Fradulently lend licence/permit
Deception/Obtain property by deception (11 offence descriptions)	• Obtain property by deception • Obtain financial advantage by deception • Make appear – goods contaminated (Crimes Act) • Receive mail by deceit • Prevent meter from registering • Supply grand prix merchandise without consent • Cause pharmacist to supply drug • Induce pharmacist to dispense prescription • Induce pharmacist supply restricted substance • Obtain drug of dependence – false representation • Obtain script drug of dependence false representation
Obtain benefit by fraud/deception (19 offence descriptions)	• Imposition-Commonwealth benefit/money • Procure certificate of title by fraud • Obtain PTC ticket by fraud • Obtain PTC concession by fraud • Bankrupt – obtain credit by fraud • Fraudulently use electricity • Fraud abstract gas from corporation • Fraudulently obtain any benefit • Attempt to fraudulently obtain benefit • Procure use of motor vehicle by fraud • Procure hire motor vehicle by fraud • Fit apparatus – unlawful gain electricity • Dishonestly procure security • Obtain licence/permit by false statement • Obtain licence by misrepresentation • Obtain registration by false statement • Unregistered tax agent receive fee • Procure use of vehicle – misrepresentation • Procure hire vehicle – misrepresentation

cont…

Category of Deception Offence (137 offence descriptions)	Listed Offence Description
Fraud (3 offence descriptions)	• Fraudulently make mixed metals • Fraudulently induce investment • Defraud Commonwealth authority
False statements (13 offence descriptions)	• False statement – prohib discharge – marine • Statement – induce belief goods contaminated • Make false statement relation to claim • Make false statement • Use false statement to induce another • Make false statement to induce another • Perjury / false declaration / false oath • Pervert course of justice (common law) • Perjury (common law) • Make false/misleading statement application • Knowlingly make a false statement • Wilfully make false statement in declaration • State false address
False information (8 offence descriptions)	• Prison visitor give false information • False misleading information – another's passport application • Obtain credit – fail disclose bankruptcy • Provide false/misleading information • False accounting • Knowingly give false information to prison officer • Knowlingly give false information • False name address EPA Act
Identity fraud / false claims (15 offence descriptions)	• Open account in false name • Unregistered doctor – claim qualified • Falsely represent to be a patentee • Fraudulently alter/use identification • Engage in legal practice without certificate • Engage legal practice without being admitted • Impersonate member CFA • Impersonate court official • Impersonate an ambulance officer • Impersonate wildlife officer • Visitor – false name address – police gaol • Carry on banking business without authority • Unregistered tax agent • Unregistered agent / act as agent • False name address Transport Act
False pretences/imposition (2 offence descriptions)	• Solicit alms under false pretences • Impose upon person-money-benefit

cont…

Category of Deception Offence (137 offence descriptions)	Listed Offence Description
Trust account deficiencies (2 offence descriptions)	• Solicitor defalcation/deficiency in account • Estate agent deficiency in trust account
Secret Commissions (4 offence descriptions)	• Secret commission – receive/solicit agent • Secret commission – give/offer to agent • Secret Commission – give/receive • Receive secret commission
Money laundering (3 offence descriptions)	• Engage in money laundering confiscation profits • Engage in money laundering Commonwealth • Engage in money laundering
Conspiracy (2 offence descriptions)	• Conspiracy to cheat/defraud (common law) • Conspiracy to defraud (common law)
Bribery (1 offence description)	• 144 Bribe public official (common Law)

Appendix C-2: Miscellaneous Fraud and Electronic Commerce-related Offence Descriptions Recorded in Victoria Police Statistics 2000-2001

Category of Offence (170 offence descriptions)	**Listed Offence Description**
Computer-related offences (4 offence descriptions)	• Unauth obstruct lawful use of computer* • Unauth interfere with computer* • Enter computer system - no authority* • Gain access to computer – no authority*
Theft (3 offence descriptions)	• Theft • Steal mail from any box/place* • Steal mail from post*
Property damage (1 offence description)	• Criminal damage-with view to gain
Obtain Drugs (2 offence descriptions)'.	• Obtain Restricted Substance - False Rep* • Obtain Drug by False Representation*
Handling stolen goods (16 offence descriptions)	• Obtain fin adv by deception* • Unlawful possession • Possess suspected stolen goods • Possess property being proceeds of crime • Possess money - being proceeds of crime • Receive property - being proceeds of crime • Receive money - being proceeds of crime • Conceal money - being proceeds of crime • Dispose property - being proceeds of crime • Bring property to Vic - proceeds of crime* • Bring money to Vic - proceeds of crime • Bring stolen goods into Victoria • Att. to dispose of stolen goods • Handle/receive/retention stolen goods • Dishonest u/take in realisatn stolen goods • Conspiracy to handle stolen goods
Justice procedures (16 offence descriptions)	• Impersonate member of police force • Cause false report to be made to police • False Info • Make false report to police • Make false statement in application • Mislead statement in application • State false name/address – Marine Act • Provide false evidence ID – Court security • Conceal offence for benefit • Refuse/fail state name/address (Crimes) • State false name/address (Crimes Act) • Fail/state false name/age/address – Gaming • Wear Uniform/badge likely to deceive • State false name when requested • State false address when requested • Offer bribe to member to forgo duty

cont…

Category of Offence (170 offence descriptions)	Listed Offence Description
Regulated public order (17 offence descriptions)	• Make false statement in liquor appl • Make misleading statement – liquor appl • Minor give false particulars • Minor supply any false evidence • Falsely represent to be over age 18 • Make false document as evidence of age • Give age docs to another person to use • Give docs to another to get proof of age • Proof of age card – falsely procure • Minor falsely represent to be 18 yrs/over • Supply false evidence age/name/address • Make false/misleading statement in appl • Interfere workings/labels gaming machine • Credit betting • Conduct any lottery-no permit • Accept bet other than money/debit bet ac • Supply any false evidence as to age
Harassment (24 offence descriptions)	• Stalk another person (Crimes Act)* • Use telecommunications service to menace • Use telecommunications service to harass • Use telecommunications service to offend • Use phone service-menace/harass/offend* • Use postal/telecom in offensive manner • Use postal service-to offend • Use postal service-menace/harass/offend • Use/possess/sell telephone intercept device • Fail report use of listening device • Open/tamper with mail (C'wealth)* • Cause mail to be wrongly delivered* • Send postal message-forged signature* • Send postal message-sign fictitious name* • Cause phone carrier supply free service* • Defraud carrier of fee payable telecomm* • Defraud phone carrier of fee/charge* • Cause phone communication be misdirected* • Tamper phone facility-hinder operation* • Knowingly interfere with a facility* • Knowingly tamper with a facility* • Recklessly interfere with a facility* • Recklessly tamper with a facility* • Interfere/tamper with phone facility*
Behaviour in public (2 offence descriptions)	• Possess article of disguise • Found disguised with unlawful intent

cont…

Category of Offence (170 offence descriptions)	**Listed Offence Description**
Pharmacy-related (10 offence descriptions)	• Utter forged prescription • Fail to retain a signed prescribed form • Induce pharmacist dispense prescription • Cause/induce pharm supply/dispense dod • Att to cause pharm dispense prescript • Att to induce pharm supply drug of dep • Induce pharm dispense drug-false rep • Cause pharm dispense drug-false rep • Cause pharm supply drug-false rep • Unauth psn-write script-pharm benefit
Transport-related (15 offence descriptions)	• Tamper with / install another odometer • Tamper / interfere with motor vehicle • Tamper with motor vehicle • Interfere with motor vehicle • Travel without valid ticket-PTC • Fail produce valid PTC ticket (Act) • Fail produce evid-PTC fare concession • Use PTC ticket/conc card-time expired • Transfer PTC ticket use to another • Fail to validate PTC ticket by machine • Assist another to evade PTC fare • Display/affix false registration plate • State false name or address • Fraud'ly alter/use veh lic/plate etc • Bribe/offer bribe officer-Transport Act
General / ancilliary (12 offence descriptions)	• Conspiracy to commit indic. offence • Incite another to commit offence • Incitement • Incitement to commit offence o/s Vic • Attempt to commit indictable offence • Conspiracy to commit indictable offence • Aid/abet another commit indict. offence • Aid/abet another commit summary offence • Aid/abet false report to police • Accessory to serious indictable offence • Install/use surveill device w/o consent • C'wealth-conspiracy-pervert justice
Conspiracy (2 offence descriptions)	• Conspire to defraud* • Collusive tendering*
Extortion/blackmail (3 offence descriptions)	• Public/threat publish libel to extort* • Blackmail* • Extortion-threat to destroy property*

cont…

Category of Offence (170 offence descriptions)	Listed Offence Description
Professionals (11 offence descriptions)	• Solicitor-Practice w/o qualifications* • Pretend to be/use title of solicitor* • Hold out/advertise as solicitor* • Practice as dentist-not registered* • False info/fraud registration as dentist* • Practice chiropody-not registered* • Unregistered doctor-carry out any act* • Unregistered doctor-take/use title* • Use title reg medical prac when not reg* • Practice as psychologist-not registered* • Advertise as psychologist-not registered*
Licences/books (3 offence descriptions)	• False info-Gaming lic/question/notice* • LMTC Make false entry in dealings book* • Remove any document from title office*
Other (29 offence descriptions)	• False statement-endanger life • Publish defamatory libel-with intent • Receive / possess proceeds of crime • Conceal / dispose proceeds of crime • Impersonate member defence forces • Impersonate returned soldier etc • WO reasonable excuse give false info • Permit use of passport by another • Possess falsified Australian passport • Make an article for sale or hire • Possess infringing article • Publish advert for copy of computer prog • Possess device for making infringing copies • Possess sound recording-purpose of trade • Wilfully give false fire alarm • Cause false fire alarm to be given • Sell goods-provide false ID • Pawn goods-provide false ID • S'hand dealer fail maintain record book • Pawnbroker fail maintain record book • Fail/mislead s'ment-s'hand/pawnb Act • Fail make accurate record of transaction • Fail to record transactions • Commercial agent-unlic-hold out as same • Make an incorrect statement • Engage in any category private Agt-unlic • Omit to furnish particulars • Furnish incorrect particulars • Destroy an article in the course of the post

cont…

Notes to Appendix C-2:

Offences marked * appear in statistics in Appendix F. The list set out here is intended to be illustrative rather than exhaustive of the range of criminal offences available to Victorian police in relation to fraud, electronic commerce and white-collar crime. Offence descriptions are given as they appear in Victoria Police statistics reports 1993–2003, although not every offence is recorded and reported every year. Offences listed here are those outside of the category of 'Deception' in the reports, although note that the Categories of Offence above are not always identical to those in the reports. Offences appearing under the 'Deception' heading in the reports are listed in Appendix C–1. The recording conventions are such that offences are also not necessarily attached to a single statutory provision, for example, the offences involving knowing and reckless interference with a phone facility, listed separately here, all come from s. 85ZJ of the *Crimes Act 1914* (Cth).

Appendix D: Official Fraud and Deception Statistics 1960-2003

Offences Recorded by Police (1)	**1960**	**1961**	**1962**	**1963**	**1964**	**1965**	**1966**	**1967**	**1968**	**1969**
Fraud offences recorded in Vic	4,277	4,763	5,541	5,427	4,531	4,549	Not Published	Not Published	5,006	4,766
Vic Population (2)	2,888,290	2,955,299	3,011,043	3,071,046	3,137,921	3,195,860	3,249,843	3,303,606	3,356,827	3,421,178
Rate/100,000 population	148	161	184	177	144	142	Not Available	Not Available	149	140
Total value stolen (£)	£217,481	£270,231	£412,791	£242,901	£284,055	£494,299	Not Recorded	Not Recorded	Not Recorded	Not Recorded
Magistrates' Court Fraud Convictions (3)	**1960**	**1961**	**1962**	**1963**	**1964**	**1965**	**1966**	**1967**	**1968**	**1969**
	43	16	516	1,184	950	1,083	1,134	1,380	1,390	1,434
Higher Courts(3) Fraud Sentences	**1960**	**1961**	**1962**	**1963**	**1964**	**1965**	**1966**	**1967**	**1968**	**1969**
Bond	25	20	31	25	40	36	46	48	55	65
Probation	10	8	7	4	29	23	21	21	22	21
Fine	0	1	0	0	2	2	2	0	8	4
< 12m custodial	33	22	17	26	43	39	48	31	36	47
> 12m custodial	8	7	13	15	28	15	9	18	19	17
Other	0	0	0	0	0	0	8	4	3	3
Total	76	58	68	70	142	115	134	122	143	157
% Custodial per total sentences	53.9	50.0	44.1	58.6	50.0	47.0	42.5	40.2	38.5	40.8
Fraud Offences of Received Offenders (4)	**1960-61**	**1961-62**	**1962-63**	**1963-64**	**1964-65**	**1965-66**	**1966-67**	**1967-68**	**1968-69**
Fraud Prisoners' Offences	1,320	1,242	1,049	1,052	1,149	992	1,093	990	1,192
All Prisoners' Offences	15,183	14,552	13,970	16,252	15,468	15,862	16,455	16,152	16,559
% Fraud per total prisoners	8.7	8.5	7.5	6.5	7.4	6.3	6.6	6.1	7.2
FraudProbationers Offences	156	80	69	95	133	189	243	298	245
All Probationers Offences	1,375	1,440	1,737	1,676	1,828	3,008	2,787	2,698	2,557
% Fraud per total probationers	11.3	5.6	4.0	5.7	7.3	6.3	8.7	11.0	9.6

cont...

Offences Recorded by Police(1)	**1970**	**1971**	**1972**	**1973**	**1974**	**1975**	**1976**	**1977**	**1978**	**1979**
Fraud offences recorded in Vic	5,964	6,506	6,759	5,169	9,777	10,333	11,291	9,600	9,680	13,836
Vic Population(2)	3,482,031	3,633,843	3,686,136	3,730,824	3,779,587	3,800,656	3,823,941	3,852,589	3,874,501	3,899,993
Rate/100,000 population	171	179	183	139	259	272	295	249	250	355
Total value stolen $	Not Recorded	1,317,651	1,965,695	1,113,275	2,325,704	2,812,109	3,025,716	4,680,736	5,847,865	5,590,902
Magistrates' Court Fraud Convictions(3)	**1970**	**1971**	**1972**	**1973**	**1974**	**1975**	**1976**	**1977**	**1978**	**1979**
	1,650	1,977	2,084	2,130	2,683	2,773	3,140	3,244	3,924 (5,527) see note (3)	7,545
Higher Courts(3) Fraud Sentences	**1970**	**1971**	**1972**	**1973**	**1974**	**1975**	**1976**	**1977**	**1978**	**1979**
Bond	64	68	82	65	58	50	35	44	28	0
Probation	28	28	30	29	18	23	19	12	0	0
Fine	4	3	8	13	19	32	15	15	9 (14) n.3	65 see n.3
< 12m custodial	45	43	42	26	37	22	20	26	25 (32) n.3	424 see n.3
> 12m custodial	13	19	11	16	13	8	5	5	10(16) n.3	26 see n.3
Other	2	3	3	0	0	1	0	1	10(56) n.3	314 see n.3
Total	156	164	176	149	145	136	94	103	82 (118) n.3	829 see n.3
% Custodial per total sentences	37.2	37.8	30.1	28.2	34.5	22.1	26.6	30.1	42.7 (40.6) n.3	54.3

cont...

Sentenced Prisoners in Custody(5)	**1970** Vic Prison Census	**1971**	**1972**	**1973** Vic Prison Census	**1974**	**1975** Vic Prison Census	**1976**	**1977** Vic Prison Census	**1978** Vic Prison Census	**1979**
Total No of Vic prisoners	2,124	Not Available	Not Available	1,739	Not Available	1,449	Not Available	1,341	1,454	1,700
No of Vic fraud prisoners	100	Not Available	Not Available	85	Not Available	52	Not Available	49	38	Not Available
% fraud prisoners per total Vic prisoners	4.71	Not Available	Not Available	4.89	Not Available	3.59	Not Available	3.65	2.61	Not Available

Fraud Offences of Received Offenders (4)	**1969-70**	**1970-71**	**1971-72**	**1972-73**	**1973-74**	**1974-75**	**1975-76**	**1976-77**	**1977-78**	**1978-79**
Fraud Prisoners' Offences	819	1,344	1,895	1,304	1,216	995	824	958	1,310	940
All Prisoners' offences	15,173	17,103	17,637	16,353	13,033	12,237	9,150	11,087	14,100	9,879
% Fraud per total prisoners	5.4	7.9	10.7	8.0	9.3	8.1	9.0	8.6	9.3	9.5
Fraud Probationers' Offences	116	56	56	265	146	104	308	249	19	450
All Probationers' Offences	2,004	1,600	1,761	2,287	1,940	1,981	2,331	2,753	3,089	4,701
% Fraud per total probationers	5.8	3.5	3.2	11.6	7.5	5.2	13.2	9.0	1.0	9.6
Fraud Attendees' Offences	-	-	-	-	-	-	-	0	12	12
All Attendees' Offences	-	-	-	-	-	-	-	183	246	339
% Fraud per total attendees	-	-	-	-	-	-	-	0	4.9	3.5

cont...

Offences Recorded by Police(1)	**1980**	**1981**	**1982**	**1983**	**1984**	**1985**	**1986-87**	**1987-88**	**1988-89**	**1989-90**	**1990-91**
Fraud Offences recorded in Vic	14,977	12,120	14,995	13,431	18,500	Not Available	42,263	62,538	64,667	42,063	50,871
VicPopulation(2)	3,930,655	3,968,398	4,012,687	4,054,498	4,097,640	4,140,421	4,183,419	4,233,557	4,261,945	4,349,711	4,406,568
Rate/100,000 population	381	305	374	331	451	Not Available	1010	1,609	1,507	967	1,154
Total Value Stolen $	Not Recorded	Not Recorded	Not Recorded	7,000,000	13,000,000	Not Recorded	Not Recorded	72,000,000	25,475,200	Not Recorded	36,767,415
Average Value Stolen $	Not Recorded	Not Recorded	Not Recorded	520	703	Not Recorded	Not Recorded	1,105	3,586	Not Recorded	2,750
Higher Criminal Courts(6)	**1980**	**1981**	**1982**	**1983**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**
ADU/Bond	303	157	85	133	194	103	111	103	68	259	165
Bond and fine	5	0	0	0	0	0	0	0	0	0	0
Super (87-91)	-	-	-	-	-	-	-	0	0	0	0
Prob (80-86)	34	80	29	57	11	24	1	-	-	-	-
Attend (80-86)	6	3	1	10	45	5	34	-	-	-	-
CSO (82-86)	-	-	0	0	5	5	14	-	-	-	-
Compsn (82-86)	-	-	0	14	0	0	0	-	-	-	-
Fine	27	41	43	99	87	32	52	30	22	28	40
Susp	-	-	-	-	-	-	-	59	68	94	125
UCW	-	-	-	-	-	-	-	42	35	28	18
ADTT/ADDP	8	0	0	0	0	0	0	24	0	24	0
CBOM	-	-	-	-	-	-	-	6	3	0	25
Other	0	0	0	0	0	0	106	1	0	0	0
Custodial < 1yr	161	210	132	93	277	220	188	361	277	365	425
Custodial 1-2yrs	76	97	89	117	51	72	38	134	85	143	153
Custodial 2-3yrs	21	59	4	27	15	64	20	27	85	19	65
Custodial 3-4yrs	3	10	3	7	20	13	26	16	0	5	7
Custodial 4-5yrs	0	6	2	16	1	5	1	17	0	0	21
Custodial 5-10yrs	19	1	0	1	2	9	1	1	0	3	1
Custodial 10+yrs	0	0	0	0	0	0	0	0	0	0	0
Sentences for all fraud offences	663	664	388	574	708	552	592	821	643	968	1,045
% Custodial per total sentences	42.2	57.7	59.3	45.5	51.7	69.4	46.3	67.7	69.5	55.3	64.3

cont...

Sentenced Prisoners in Custody(5)	**1980** Vic Prison Census	**1981**	**1982**	**1983**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**
Total No of Vic prisoners	1,571	1,637	1,753	1,996	1,845	1,879	1,955	1,956	2,071	2,256	2,316
No of Vic fraud prisoners	62	Not Available	53	69	59	40	54	73	77	64	62
% fraud prisoners per total Vic prisoners	3.95	Not Available	3.02	3.46	3.20	2.13	2.76	3.73	3.72	2.84	2.68
Total No of Aust prisoners	Not Available	Not Available	9,826	10,196	9,694	10,844	11,497	12,113	12,321	12,964	14,305
No of Aust fraud prisoners	Not Available	Not Available	434	475	406	424	495	549	543	534	604
% fraud prisoners per total Aust prisoners	Not Available	Not Available	4.42	4.66	4.19	3.91	4.31	4.53	4.41	4.12	4.22
Fraud Offences of Received Offenders to 1984-85(4)	**1979-80**	**1980-81**	**1981-82**	**1982-83**	**1983-84**	**1984-85**	**1986**	**1987**	**1988**	**1989**	**1990**
Fraud Prisoners' Offences	1,157	2,230	2,019	3,409	4,328	4,506	NA	67	72	59	57
All Prisoners' Offences	12,205	17,045	17,240	22,709	28,922	28,148	1,751 stock	1,707 stock	1,824	1,956	1,954
% Fraud per total prisoners	9.5	13.1	11.7	15.0	15.0	16.0	NA	3.9	3.9	3.0	2.9
Fraud Probationers' Offences	863	1,204	1,782	1,451	1,722	2,198	NA	NA	49	15	11
All Probationers' Offences	5,043	5,566	6,234	7,456	7,580	8,187	9,744 flow	1,653 stock	456	202	145
% Fraud per total probationers	17.1	21.6	28.6	19.5	22.7	26.8	NA	NA	10.7	7.4	7.6
Fraud Attendees' Offences	10	107	45	97	329	888	NA	NA	-	-	-
All Attendees' Offences	298	926	1,759	1,894	2,108	2,584	3,504 flow	4 stock	-	-	-
% Fraud per total attendees	3.4	11.6	2.6	5.1	15.6	34.4	NA	NA	-	-	-
Fraud CSO/CBC Offences	-	-	-	1 (pt yr)	2	149	NA	NA	400	403	392
All CSO/CBC Offences	-	-	-	50 (pt yr)	79	982	5,495 flow	3,375 stock	3,919	3,726	3,811
% Fraud per total CSO/CBC Offences	-	-	-	2.0	2.5	15.2	NA	NA	10.2	10.8	10.3
Fraud Interstate/Cth Offences	-	-	-	-	-	-	-	NA	10	31	10
All Interstate/Cth offences	-	-	-	-	-	-	-	64 stock	66	127	169
% Fraud per total Inter/Cth Offences	-	-	-	-	-	-	-	NA	15.2	24.4	5.9
Sentenced Offenders on CBOs(7)	**1980**	**1981**	**1982**	**1983**	**1984**	**1985** CBO Census	**1986**	**1987** CBO Census	**1988**	**1989** CBO Census	**1990**
Total No of Vic CBO offenders	Not Available	Not Available	4,207	4,246	4,950	5,177	6,434	5,937	5,838	5,181	5,264
No of Vic fraud CBO offenders	Not Available	Not Available	Not Available	Not Available	Not Available	465	Not Available	607	Not Available	488	Not Available
% Vic fraud offenders per total Vic CBOs	Not Available	Not Available	Not Available	Not Available	Not Available	8.98	Not Available	10.2	Not Available	9.4	Not Available
Total No of Aust CBO offenders	Not Available	Not Available	Not Available	Not Available	Not Available	31,403	Not Available	37,794	Not Available	39,921	Not Available
No of Aust fraud CBO offenders	Not Available	Not Available	Not Available	Not Available	Not Available	2,683	Not Available	3,345	Not Available	3,377	Not Available
% fraud offenders per total Aust CBOs	Not Available	Not Available	Not Available	Not Available	Not Available	8.5	Not Available	8.9	Not Available	8.5	Not Available

cont...

Offences Recorded by Police(1)	**1991-92**	**1992-93**	**1-3-93** *LEAP began*	**1993-94**	**1994-95**	**1995-96**	**1996-97**	**1997-98**	**1998-99**	**1999-00**	**2000-01**	**2001-02**	**2002-03**
Fraud Offences recorded in Vic	47,681	41,955		25,082	26,718	29,805	32,773	35,191	38,021	37,270	29,753	28,506	28,933
VicPopulation(2)	4,437,500	4,465,415		4,478,835	4,500,354	4,539,796	4,583,445	4,627,399	4,684,082	4,738,181	4,854,196	4,902,920	4,929,750
Rate/100,000 population	1,077	942		562	597	659	714	761	812	787	613	581	587
Total Value Stolen $	54,407,144	34,798,493		*Not Recorded*	38,687,092	45,127,000	43,929,000	117,263,000	553,992,000	24,027,806	1,371,957	1,410,592	1,824,989
Average Value Stolen $	3,926	2,676		*Not Recorded*	2,619	3,225	4,904	7,194	31,859	7,555	3,076	2,141	2,883
Magistrates' Court(8)				**1994**	**1995**	**1996**	**1997**	**1997-98**	**1998-99**	**1999-00**	**2000-01**	**2001-02**	**2002-03**
No of principal proven fraud offences	*Not Available*	*Not Available*		3,222	2,625	2,382	2,372	2,496	2,629	*Not Available*	*Not Available*	*Not Available*	*Not Available*
Custodial								267	215				
Suspended								209	202				
ICO								66	60				
CBO								355	301				
Bond								450	483				
Fine								1,148	1,365				
Conv & disch								1	3				
Higher Criminal Courts(6)	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**//**	**1997-98**	**1998-99**	**1999-00**	**2000-01**	**2001-02**	**2002-03**
ADU/Bond	133	28	18	8	52	10		50	37	47	58	36	
ICO (>92)	-	28	0	0	2	14		6	5	2	3	5	
Fine	29	11	4	6	4	4		4	7	3	8	6	
Susp	261	144	183	166	319	184		29	43	49	52	55	
UCW	89	17	60	25	21	29		-	-	-	-	-	
ADTT/ADDP	0	0	1	0	0	1		-	-	-	-	-	
CBOM	12	1	0	0	2	1		6	3	12	8	7	
Other	0	0	2	0	0	9		1	-	4	3	2	
Custodial < 1yr	124	214	129	169	76	231		21	26	37	24	18	
Custodial 1-2yrs	104	195	165	170	24	98		11	13	18	22	18	
Custodial 2-3yrs	28	74	86	145	23	34		6	3	3	8	6	
Custodial 3-4yrs	9	24	21	6	4	25		3	1	5	2	1	
Custodial 4-5yrs	24	11	20	3	1	8		2	1	2	-	2	
Custodial 5-10yrs	2	1	7	1	1	0		2	-	1	-	-	
Custodial 10+yrs	0	0	0	0	1	0	-	-	-	-	-		
Sentences for all fraud offences	815	748	696	699	530	648		141	139	183	188	156	
%age custodial per total sentences	35.7	69.4	61.5	70.7	24.5	61.1		31.9	31.6	35.5	29.8	28.8	*Not Available*

cont...

Sentenced Prisoners in Custody(5)	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002
Total No of Vic prisoners	2,310	2,277	2,277	2,189	2,118	2,058	2,226	2,422	2,506	2,717	2,892	3,540
No of Vic fraud prisoners	75	78	81	98	94	90	85	77	86	94	81	80
% fraud prisoners per total Vic prisoners	3.25	3.43	3.56	4.48	4.44	4.38	3.82	3.18	3.43	3.46	2.80	2.26
Total No of Aust prisoners	15,021	15,559	15,866	14,998	15,429	15,887	16,522	17,118	18,332	17,929	18,123	22,492
No of Aust fraud prisoners	563	549	691	709	700	690	753	682	723	635	574	555
% fraud prisoners per total Aust prisoners	3.75	3.53	4.36	4.73	4.54	4.34	4.56	3.98	3.94	3.54	3.17	2.47

Fraud Offences of Received Offenders (4)	1991	1992
Fraud Prisoners' Offences	70	69
All Prisoners' Offences	1,925	1,911
% Fraud per total prisoners	3.6	3.6
Fraud Probationers' Offences	4	-
All Probationers' Offences	59	-
% Fraud per total probationers	6.8	-
Fraud CBO Offences	494	565
All CBO Offences	5,309	6,201
% Fraud per total CSO/CBC Offences	9.3	9.1
Fraud Interstate/Cth Offences	12	-
All Interstate/Cth offences	210	-
% Fraud per total Inter/Cth Offences	5.7	-
Fraud ICO offences	-	10
All ICO offences	-	113
% Fraud per total ICO Offences	-	8.8

NOTES TO ALL TABLES IN APPENDIX D:

Sources: (1) Victoria Police Statistical Review and, after and including 1993-94, information from Victoria Police Law Enforcement Assistance Program database implemented on 1-3-93. Counting rules changed with the implementation of LEAP in 1993.

(2) Victorian population statistics are taken from Australian Bureau of Statistics, *Victorian Year Book*, Melbourne recorded at 31 December each year, except for 2002-03 which is at 31 March 2003.

(3) Court statistics derived from *Victorian Yearbooks*, Commonwealth Bureau of Census and Statistics, Victorian Office, Melbourne.

1960-1961 Offences of forgery and offences against currency only (Magistrates' Courts)

1960-1962 Offences of Embezzlement, false pretences, and fraudulent conversion (Higher Courts – County Court and Supreme Court)

1963-1977 Offences of fraud, forgery and false pretences (Magistrates' Courts and Higher Courts – County Court and Supreme Court)

1978 – Categorisation changed from fraud, forgery and false pretences (1963-77) to fraud and deception 1978- using (draft) ANCO categorisation. This resulted in an increase in the number of convictions recorded (e.g. Higher Courts in 1978 from 82 to 115 convictions).

1979 - Supreme Court statistics did not have a separate category for fraud and deception and so are excluded – In 1979 only County Court convictions noted.

After 1979, *Yearbook* court statistics only used the category breaking and entering, fraud, and other theft.

Sentencing abbreviation of BOND is sentence suspended on entering into a bond.

(4) Fraud Offences of Received Offenders (Flow) – Sentenced offenders only - From *Annual Reports* Social Welfare Department 1962-78, Department of Community Welfare Services 1978-82, Office of Corrections 1983-1992 for adult offenders received into prison or placed on probation etc. during each financial year for most serious offence of false pretences. After 1979-80 most serious offence of fraud and misappropriation. Attendance Centres commenced June 1976, Community Service Orders commenced September 1982, Pre-release Program commenced April 1984.

From 1986, Office of Corrections statistics record offenders in custody at 30 June each year. Statistics for sentenced prisoners only are included above. CBO – Community Based Orders including orders following a period of imprisonment and in default of payment of fines (fine conversion). Interstate/Cth - Interstate and Commonwealth offenders on CBC/CBOs. Parole and Pre-Release are excluded.

(5) Total No of Vic Prisoners - Sentenced and Unsentenced prisoners in custody in Victoria for most serious offence of fraud and misappropriation Australian Bureau of Statistics *Prisoners in Australia* at 30 June each year (National Prison Census figures for Prison Stock).

Fraud Offences of Received offenders – Sentenced offenders only - Office of the Correctional Services Commissioner *Statistical Profile The Victorian Prison System*, Department of Justice, Melbourne. Prisoners at 30 June each year.

Victorian Prison Censuses conducted on the evenings of 17-18 October 1970, 27-28 October 1973, 25-26 October 1975, 22-23 October 1977, October 1978, 25-26 October 1980,26-27 June 1982.

(6) Sentencing Statistics Higher Criminal Courts Victoria

1980 to 1996 - (Published by Courts and Tribunals Services Division, Department of Justice, Melbourne). Offences relating to fraud and deception are within category 6.1, and fraud and deception-related conspiracy offences in category 8.4. The definitions of these offences varied over time, along with their descriptions but they include: Obtaining property by deception, attempt to obtain property by deception, obtain financial advantage by deception, attempt to obtain financial advantage by deception, false accounting, secret commissions or bribery, attempted bribery, possession of articeles of disguise, forgery, uttering, unlicensed securities dealer, procuring the execution of a valuable security by deception, fraudulently inducing persons to invest, fraud, false pretence, trust account deficiency, defalcation by a solicitor, improper use of position as officer in corporation, fraudulent conversion, falsifying records, furnish false information, make false document, use false document, conspire to make false statements or birth certificates, falsify passport, conspire to defraud, conspire to obtain property by deception (some involved multiple sentences). Some possibly relevant offences are not included such as theft and accessory offences. Not each of these offences were dealt with each year.

1997-98 to 2001-02 (Published by Court Services, Department of Justice, Melbourne: http://www.justice.vic.gov.au/CA256902000FE154/Lookup/VHC_Stats_Vol_One_PartB_12_jun_2003.pdf/$file/VHC_Stats_Vol_One_PartB_12_jun_2003.pdf)

These statistics are not directly comparable to those presented for previous years. Details of the

counting rules and definitions for 1997-98 to 2001-02 are available at:
http://www.justice.vic.gov.au/CA2569020010922A/page/Resources-Statistics+and+Facts-Victorian+Higher+Courts+Sentencing+Statistics+1997-98+to+2001-02?OpenDocument&1=0-Resources~&2=0-Statistics+and+Facts~&3=0-Victorian+Higher+Courts+Sentencing+Statistics+1997-98+to+2001-02~

See sentence abbreviations below. (7) Australian Community-based Corrections Censuses conducted in Victoria on 30-9-85, 30-6-87 and 30-6-89 published by Australian Institute of Criminology.

Note: Amendments were made to Victorian Community-based Orders on 1 June 1986. Most serious offence of fraud and misappropriation (1985, 1987) based on (draft) ANCO at the relevant time. Statistics on total number of CBO offenders for non-Census years are from *Victorian Yearbooks*.

(8) Statistics of the Magistrates' Court of Victoria, Department of Justice, Melbourne

For 1997-98 to 1998-99 Deception Offences – principal proven offence

For 1994-1997 Sentenced offences of fraud, forgery, false pretences, misappropriation, and counterfeiting.

Magistrates' Court statistics published from 1990 onwards but no ANCO classification until 1994 and no sentencing breakdown x ANCO categorisation until 1997-98. Series held at Office of the Correctional Services Commissioner finishes at 1998-99.

Offence Categories

Offence categories based on Australian Standard Classification of Offences after 1997 (ASCO) Category (deception and related offences) and Australian National Classification of offences from 1985 (ANCO) Category (fraud and misappropriation).

Specific classification terms used in official tables include:

1993-94 to 2000-01 Deception Offences recorded by Police

1986-87 to 1992-93 Fraudulent Offences recorded by Police (Deception and currency offences)

1978 to 84 Calendar years (Fraud etc)

1974 to 77 Calendar years (Obtain by deception, offences against trust/currency)

1973 Fraud, forgeries, false pretences (includes all moffences of trsusteeship, false pretences, currency or attempted, but excludes imposition).

1972 Fraud, forgeries, false pretences (includes all offences of trsusteeship, false pretences, currency or attempted, including imposition).

Value Stolen

1960-65 Value was published in (£) pounds for larceny by a trick, imposition, false pretences, false pretences (cheques) Does not include all offences as some the value was not stated or not known..

After 14-2-1966 value in ($) dollars.

Years Recorded

1960 to 1984 Calendar years 1 January to 31 December shown above as **1960 etc**

1986-87 to 2000-2003 Financial years 1 July to 30 June show above as **86-87 etc**

NB Obtain property by deception is the second most common offence in Magistrates' Courts 1998-99 7.8% of all offences (23,056 out of 296,000 top 100 most common offences).

Sentence Abbreviations:

1997-98 to 2001-02

ADU/BOND - Adjourned undertaking or common law bond including s. 20(1)(b) Commonwealth bond

ICO - Intensive corrections order

FINE - Fine

SUSP - Suspended sentence of imprisonment

CBOM - Community based order

CUSTODIAL – Imprisonment: < 1 - Twelve months or less

1992-1996
ADU/BOND - Adjourned undertaking or common law bond
ICO - Intensive corrections order
FINE - Fine
SUSP - Suspended sentence of imprisonment
UCW - Community based order unpaid community work
ADTT - Community based order - Assessment and treatment for alcohol or drug addiction or submit to medical, psychological or psychiatric assessment and treatment
CBOM - Other Community based orders
CUSTODIAL – Prison or Youth Training Centre: < 1 - Twelve months or less

1987-1991
SUPER - Supervision by a community corrections officer
FINE - fine
UCW - CBO unpaid community work
ADTT - CBO assessement etc
CBOM - Other CBOs
CUSTODIAL – Prison or Youth Training Centre: < 1 - Twelve months or less

1982-1986
BOND - Common law bond
PROB - Probation
ATTEND - Attendance Centre
CSO - Community Service Order
ADDP - Alcohol and Drug Dependent Persons Act 1968 orders
COMPSN – Compensation orders
CUSTODIAL – Prison or Youth Training Centre: < 1 - Twelve months or less

1976-1981
BOND - Includes bond and fine
PROB – Includes probabtion or probation and fine
ATTEND/ADDP - Attendance centre or ADDP order

Appendix E: Number of Deception Offences where Property was Recorded as Stolen/Affected by Year, Offence Type and Value Range of Property Affected 1996-1997 to 2002-2003

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 1996/97 Offence description		Number of offences recorded per $ value range Statutory reference					
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	1,859	182	234	76	4	2,153,782
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	0	0	0	0
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	47	28	10	18	1	135,618
FORGE C'WEALTH DOCUMENT	*Crimes Act* 1914 (Cth) s. 67	1	0	0	0	0	50
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	0	0	0	0	0	0
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	2	1	0	0	0	650
POSSESS GOODS FOR SALE- FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(c)	0	0	0	0	0	0
USE FALSE DOCUMENT (CRIMES ACT)	s. 83A(2)	0	0	0	0	0	0
USE COPY OF FALSE DOCUMENT (CRIMES ACT)	s. 83A(4)	0	0	0	0	0	0
PROCURE USE/HIRE VEHICLE BY FRAUD/MISREP	*Road Safety Act* 1986 (Vic) s. 69(a)	2	0	0	0	0	695
PROCURE USE OF MOTOR VEHICLE BY FRAUD	As above	0	0	0	0	0	0
FALSE ACCOUNTING	s. 83(1)(a)	0	0	0	0	0	0
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE HIRE VEHICLE - MISREPRESENTATION	As above	0	0	0	0	0	0
INTENT. FALSELY APPLY REG TRADEMARK	*Trade Marks Act* 1995 (Cth) s. 146(1)(a)	0	0	0	0	0	0
POSS GOODS FOR MANFACT FALSE TRADEMARK	As above s. 148(c)	0	0	0	0	0	0
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	0	0	0	0	0	0

cont...

(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
UTTER DOCUMENT ISSUABLE TO COMMONWEALTH	*Crimes Act* 1914 (Cth) s. 67(b)	0	0	0	0	0	0
SOLICITOR-DEFALCATION-DEFICIENT IN ACCNT	*Legal Profession Practice Act* 1958 (Vic) s. 42(1)	0	0	0	0	0	0
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	0	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	7	0	1	0	0	4,207
BUY/SELL/REC/DISPOSE COUNTERFEIT MONEY	As above s. 8(1)	1	0	0	0	0	0
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	0	0	0	0	0	0
STEAL/FRAUD CONCEAL/DESTROY POST MESSAGE	*Crimes Act* 1914 (Cth) s. 85P	1	0	0	0	0	400
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	0	0	0	0	0	0
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	2	0	0	0	0	0
OBTAIN SCRIPT FOR RESTR SUBST-FALSE REP	As above s. 36B(1)(b)	0	0	0	0	0	0
FRAUDULENTLY ALTER PRESCRIPTION	As above s. 36A	1	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	0	0	0	0	0	0
CAUSE PHARM DISPENSE PRESC REST SUBST	As above s. 36B(1)(d)	1	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	0	0	0	0	0	0
OBTAIN DRUG OF DEPENDENCE-FALSE REPRESEN	As above s. 78(a)	0	0	0	0	0	0
OBTAIN SCRIPT DRUG DEPENDENCE-FALSE REP	As above s. 78(b)	0	0	0	0	0	0
Total deception		**1,924**	**211**	**245**	**94**	**5**	**2,295,401**

Data extracted from LEAP on 29 August 2002

Produced by Statistical Services Division

cont...

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 1997/98		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	937	274	649	35	0	883,519
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	1	0	0	1300
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	31	6	27	0	0	32,037
FORGE C'WEALTH DOCUMENT	*Crimes Act* 1914 (Cth) s. 67	1	0	0	0	0	0
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	0	0	0	0	0	0
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	3	0	0	0	0	280
POSSESS GOODS FOR SALE- FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(c)	0	0	0	0	0	0
USE FALSE DOCUMENT (CRIMES ACT)	s. 83A(2)	1	0	0	0	0	100
USE COPY OF FALSE DOCUMENT (CRIMES ACT)	s. 83A(4)	0	0	0	0	0	0
PROCURE USE/HIRE VEHICLE BY FRAUD/MISREP	*Road Safety Act* 1986 (Vic) s. 69(a)	3	0	1	0	0	1,162
PROCURE USE OF MOTOR VEHICLE BY FRAUD	As above	0	0	0	0	0	0
FALSE ACCOUNTING	s. 83(1)(a)	1	0	0	0	0	0
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE HIRE VEHICLE - MISREPRESENTATION	As above	0	0	0	0	0	0
INTENT. FALSELY APPLY REG TRADEMARK	*Trade Marks Act* 1995 (Cth) s. 146(1)(a)	0	0	0	0	0	0
POSS GOODS FOR MANFACT FALSE TRADEMARK	As above s. 148(c)	0	0	0	0	0	0

cont...

(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	0	0	0	0	0	0
UTTER DOCUMENT ISSUABLE TO COMMONWEALTH	*Crimes Act* 1914 (Cth) s. 67(b)	0	0	0	0	0	0
SOLICITOR-DEFALCATION-DEFICIENT IN ACCNT	*Legal Profession Practice Act* 1958 (Vic) s. 42(1)	0	0	0	0	0	0
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	1	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	2	0	0	0	0	120
BUY/SELL/REC/DISPOSE COUNTERFEIT MONEY	As above s. 8(1)	2	0	0	0	0	100
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	0	0	0	0	0	0
STEAL/FRAUD CONCEAL/DESTROY POST MESSAGE	*Crimes Act* 1914 (Cth) s. 85P	0	0	0	0	0	0
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	0	0	0	0	0	0
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	5	0	0	0	0	10
OBTAIN SCRIPT FOR RESTR SUBST-FALSE REP	As above s. 36B(1)(b)	0	0	0	0	0	0
FRAUDULENTLY ALTER PRESCRIPTION	As above s. 36A	2	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	0	0	0	0	0	0
CAUSE PHARM DISPENSE PRESC REST SUBST	As above s. 36B(1)(d)	0	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	1	0	0	0	0	0
OBTAIN DRUG OF DEPENDENCE-FALSE REPRESEN	As above s. 78(a)	0	0	0	0	0	0
OBTAIN SCRIPT DRUG DEPENDENCE-FALSE REP	As above s. 78(b)	1	0	0	0	0	0
Total deception		**991**	**280**	**678**	**35**	**0**	**918,628**

Data extracted from LEAP on 29 August 2002

Produced by Statistical Services Division

cont...

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 1998/99		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	690	222	249	22	12	1,366,494
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	0	0	0	0
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	62	12	13	3	0	86,214
FORGE C'WEALTH DOCUMENT	*Crimes Act* 1914 (Cth) s. 67	0	0	0	0	0	0
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	4	0	0	0	0	0
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	4	0	0	0	0	0
POSSESS GOODS FOR SALE- FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(c)	2	0	0	0	0	180
USE FALSE DOCUMENT (CRIMES ACT)	s. 83A(2)	0	0	0	0	0	0
USE COPY OF FALSE DOCUMENT (CRIMES ACT)	s. 83A(4)	8	0	0	0	0	1,765
PROCURE USE/HIRE VEHICLE BY FRAUD/MISREP	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE USE OF MOTOR VEHICLE BY FRAUD	As above	0	0	0	0	0	0
FALSE ACCOUNTING	s. 83(1)(a)	0	0	0	0	0	0
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE HIRE VEHICLE - MISREPRESENTATION	As above	0	0	0	0	0	0
INTENT. FALSELY APPLY REG TRADEMARK	*Trade Marks Act* 1995 (Cth) s. 146(1)(a)	0	0	0	0	0	0
POSS GOODS FOR MANFACT FALSE TRADEMARK	As above s. 148(c)	0	0	0	0	0	0
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	2	0	0	0	0	0

cont...

(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
UTTER DOCUMENT ISSUABLE TO COMMONWEALTH	*Crimes Act* 1914 (Cth) s. 67(b)	0	0	0	0	0	0
SOLICITOR-DEFALCATION-DEFICIENT IN ACCNT	*Legal Profession Practice Act* 1958 (Vic) s. 42(1)	0	0	0	0	0	0
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	0	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	3	0	0	0	0	70
BUY/SELL/REC/DISPOSE COUNTERFEIT MONEY	As above s. 8(1)	0	0	0	0	0	0
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	0	0	0	0	0	0
STEAL/FRAUD CONCEAL/DESTROY POST MESSAGE	*Crimes Act* 1914 (Cth) s. 85P	0	0	0	0	0	0
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	3	0	0	0	0	0
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	5	0	0	0	0	100
OBTAIN SCRIPT FOR RESTR SUBST-FALSE REP	As above s. 36B(1)(b)	1	0	0	0	0	0
FRAUDULENTLY ALTER PRESCRIPTION	As above s. 36A	0	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	1	0	0	0	0	0
CAUSE PHARM DISPENSE PRESC REST SUBST	As above s. 36B(1)(d)	0	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	4	0	0	0	0	6
OBTAIN DRUG OF DEPENDENCE-FALSE REPRESEN	As above s. 78(a)	1	0	0	0	0	0
OBTAIN SCRIPT DRUG DEPENDENCE-FALSE REP	As above s. 78(b)	0	0	0	0	0	0
Total deception		**790**	**234**	**262**	**25**	**12**	**1,454,829**

Data extracted from LEAP on 29 August 2002

Produced by Statistical Services Division

cont...

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 1999/00		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	1316	455	228	28	6	1,341,676
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	0	0	0	0
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	56	3	2	1	0	29,183
FORGE C'WEALTH DOCUMENT	*Crimes Act* 1914 (Cth) s. 67	0	0	0	0	0	0
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	0	0	0	0	0	0
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	4	0	0	0	0	30
POSSESS GOODS FOR SALE- FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(c)	0	0	0	0	0	0
USE FALSE DOCUMENT (CRIMES ACT)	s. 83A(2)	0	0	0	0	0	0
USE COPY OF FALSE DOCUMENT (CRIMES ACT)	s. 83A(4)	0	0	0	0	0	0
PROCURE USE/HIRE VEHICLE BY FRAUD/MISREP	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE USE OF MOTOR VEHICLE BY FRAUD	As above	0	0	0	0	0	0
FALSE ACCOUNTING	s. 83(1)(a)	0	0	0	0	0	0
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	3	0	0	0	0	522
PROCURE HIRE VEHICLE - MISREPRESENTATION	As above	0	0	0	0	0	0
INTENT. FALSELY APPLY REG TRADEMARK	*Trade Marks Act* 1995 (Cth) s. 146(1)(a)	110	0	0	0	0	0
POSS GOODS FOR MANFACT FALSE TRADEMARK	As above s. 148(c)	5	0	0	0	0	0
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	0	0	0	0	0	0

cont...

(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
UTTER DOCUMENT ISSUABLE TO COMMONWEALTH	*Crimes Act* 1914 (Cth) s. 67(b)	0	25	0	0	0	4,515
SOLICITOR-DEFALCATION-DEFICIENT IN ACCNT	*Legal Profession Practice Act* 1958 (Vic) s. 42(1)	0	0	0	0	0	0
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	1	0	0	0	0	50
UTTER COUNTERFEIT MONEY	As above s. 7(a)	1	0	0	0	0	0
BUY/SELL/REC/DISPOSE COUNTERFEIT MONEY	As above s. 8(1)	0	0	0	0	0	0
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	3	0	0	0	0	70
STEAL/FRAUD CONCEAL/DESTROY POST MESSAGE	*Crimes Act* 1914 (Cth) s. 85P	0	0	0	0	0	0
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	0	0	0	0	0	0
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	2	0	0	0	0	10
OBTAIN SCRIPT FOR RESTR SUBST-FALSE REP	As above s. 36B(1)(b)	0	0	0	0	0	0
FRAUDULENTLY ALTER PRESCRIPTION	As above s. 36A	1	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	0	0	0	0	0	0
CAUSE PHARM DISPENSE PRESC REST SUBST	As above s. 36B(1)(d)	0	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	0	0	0	0	0	0
OBTAIN DRUG OF DEPENDENCE-FALSE REPRESEN	As above s. 78(a)	0	0	0	0	0	0
OBTAIN SCRIPT DRUG DEPENDENCE-FALSE REP	As above s. 78(b)	0	0	0	0	0	0
Total deception		**1,502**	**483**	**230**	**29**	**6**	**1,376,056**

Data extracted from LEAP on 29 August 2002

Produced by Statistical Services Division

cont...

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 2000/01		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	1,225	328	268	35	3	1,916,401
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	0	0	0	0
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	133	10	6	0	0	26,333
FORGE C'WEALTH DOCUMENT	*Crimes Act* 1914 (Cth) s. 67	0	0	0	0	0	0
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	0	0	0	0	0	0
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	7	0	1	0	0	3,550
POSSESS GOODS FOR SALE- FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(c)	0	0	0	0	0	0
USE FALSE DOCUMENT (CRIMES ACT)	s. 83A(2)	0	0	0	0	0	0
USE COPY OF FALSE DOCUMENT (CRIMES ACT)	s. 83A(4)	0	0	0	0	0	0
PROCURE USE/HIRE VEHICLE BY FRAUD/MISREP	*Road Safety Act* 1986 (Vic) s. 69(a)	0	0	0	0	0	0
PROCURE USE OF MOTOR VEHICLE BY FRAUD	As above	2	0	0	0	0	24
FALSE ACCOUNTING	s. 83(1)(a)	0	0	0	0	0	0
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	3	0	0	0	0	606
PROCURE HIRE VEHICLE - MISREPRESENTATION	As above	1	0	0	0	0	170
INTENT. FALSELY APPLY REG TRADEMARK	*Trade Marks Act* 1995 (Cth) s. 146(1)(a)	0	0	0	0	0	0
POSS GOODS FOR MANFACT FALSE TRADEMARK	As above s. 148(c)	0	0	0	0	0	0
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	0	0	0	0	0	0

cont...

(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		< $500	$501 - $1,000	$1,001 - $10,000	$10,001 - $50,000	> $50,000	Total value ($)
UTTER DOCUMENT ISSUABLE TO COMMONWEALTH	*Crimes Act* 1914 (Cth) s. 67(b)	0	0	0	0	0	0
SOLICITOR-DEFALCATION-DEFICIENT IN ACCNT	*Legal Profession Practice Act* 1958 (Vic) s. 42(1)	0	0	0	0	1	685,400
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	0	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	5	0	0	0	0	200
BUY/SELL/REC/DISPOSE COUNTERFEIT MONEY	As above s. 8(1)	1	0	0	0	0	100
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	2	0	0	0	0	150
STEAL/FRAUD CONCEAL/DESTROY POST MESSAGE	*Crimes Act* 1914 (Cth) s. 85P	0	0	0	0	0	0
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	1	0	0	0	0	0
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	1	0	0	0	0	25
OBTAIN SCRIPT FOR RESTR SUBST-FALSE REP	As above s. 36B(1)(b)	0	0	0	0	0	0
FRAUDULENTLY ALTER PRESCRIPTION	As above s. 36A	0	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	0	0	0	0	0	0
CAUSE PHARM DISPENSE PRESC REST SUBST	As above s. 36B(1)(d)	0	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	0	0	0	0	0	0
OBTAIN DRUG OF DEPENDENCE-FALSE REPRESEN	As above s. 78(a)	0	0	0	0	0	0
OBTAIN SCRIPT DRUG DEPENDENCE-FALSE REP	As above s. 78(b)	0	0	0	0	0	0
Total deception		**1,381**	**338**	**275**	**35**	**4**	**2,632,959**
Data extracted from LEAP on 29 August 2002							
Produced by Statistical Services Division							

NOTE:

These tables only include offence descriptions for which a value was recorded for the property stolen or affected (i.e. only 33 offence descriptions out of the 137 total offence descriptions noted above in Appendix C.

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 2001/02		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	285	87	140	16	68	1,335,052
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	19	2	9	15	0	32,066
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	1	0	1	1	0	37,215
PROCURE HIRE OF MOTOR VEHICLE BY FRAUD	*Road Safety Act* 1986 (Vic) s. 69(a)	1	0	0	0	0	45
PROCURE/USE ACCOUNT TO MISLEAD/DECEIVE	s. 83(1)B	0	0	1	0	0	5,965
ENGAGE IN MONEY LAUNDERING	*Confiscation Act* 1997 s. 122(1)	1	0	0	0	0	0
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	1	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	7	0	0	0	0	150
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	1	0	0	0	0	100
FORGE PRESCRIPTION-DRUG OF DEPENDENCE	As above s. 77	1	0	0	0	0	0
UTTER FORGED SCRIPT- RESTRICTED SUBSTANCE	As above	1	0	0	0	0	0
UTTER FORGED SCRIPT- DRUG OF DEPENDENCE	As above s. 77	1	0	0	0	0	0
Total deception		**319**	**89**	**151**	**32**	**68**	**1,410,592**

Data extracted from LEAP on 13 October 2003

Produced by Statistical Services Division

Number of deception offences where property was recorded as stolen/affected by year, offence type and value range of property affected.

FINANCIAL YEAR 2002/03		Number of offences recorded per $ value range					
Offence description	**Statutory reference**						
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)		**< $500**	**$501 - $1,000**	**$1,001 - $10,000**	**$10,001 - $50,000**	**> $50,000**	**Total value ($)**
OBTAIN PROPERTY BY DECEPTION	s. 81(1)	280	96	135	46	2	1,773,982
OBTAIN GOODS BY VALUELESS CHEQUE	*Summary Offences Act* 1966 s. 37(1)	0	0	1	0	0	1,950
OBTAIN FINANCIAL ADVANTAGE BY DECEPTION	s. 82(1)	29	1	21	0	0	36,950
EXPOSE GOODS FOR SALE-FORGED TRADE MARK	*Trade Marks Act* 1955 (Cth) s. 99(1)(b)	7	0	7	0	0	11,000
MAKE FALSE DOCUMENT (CRIMES ACT)	s. 83A(1)	2	0	0	0	0	0
HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)	s. 83A(5)	1	0	0	0	0	500
PROCURE/USE ACCOUNT TO MISLEAD/DECEIVE	s. 83(1)B	1	0	0	0	0	357
MAKE COUNTERFEIT MONEY	*Crimes (Currency) Act* 1981 (Cth) s. 6	1	0	0	0	0	0
UTTER COUNTERFEIT MONEY	As above s. 7(a)	1	0	0	0	0	50
POSSESS COUNTERFEIT MONEY	As above s. 9(1)(a)	2	0	0	0	0	200
FORGE PRESCRIPTION-RESTRICTED SUBSTANCE	*Drugs, Poisons and Controlled Substances Act* 1981 (Vic) s. 36A	1	0	0	0	0	0
Total deception		**325**	**96**	**164**	**46**	**2**	**1,824,989**
Data extracted from LEAP on 13 October 2003							
Produced by Statistical Services Division							

NOTE:

These tables only include offence descriptions for which a value was recorded for the property stolen or affected (i.e. only 33 offence descriptions out of the 137 total offence descriptions noted above in Appendix C).

Appendix F: Number of Miscellaneous Fraud and Electronic Commerce-related Offences Recorded by Police 1993-94 to 2002-2003

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001	2001-2002	2002-2003
Computer-related offences											
Unauth Obstruct lawful use of computer (Other)	Crimes Act 1914 (Cth) s. 76E(b)	-	-	-	-	-	N/A	0	1	1	0
Unauth Interfere with computer (Other)(1)	As above	-	-	-	-	-	71	0	3	2	1
Enter computer system – no authority (Other)	Summary Offences Act 1966 (Vic) s. 9A	1	6	1	31	13	61	19	6	20	5
Gain access to computer – no authority (Other)	As above	1	0	1	1	3	14	5	43	13	9
Extortion/blackmail											
Publish/threat publish libel to extort (Other)	Wrongs Act 1958 (Vic) s. 9	0	0	0	0	1	1	0	0	0	1
Blackmail (Other)	s. 87	91	129	64	89	114	93	76	93	99	145
Extortion-threat to destroy property (Other)	s. 28	1	3	1	8	13	2	3	1	9	2
Professionals											
Solicitor-Practice w/o qualifications (Other)	Legal Profession Practice Act 1958 (Vic) s. 90(6)	0	6	2	1	0	8	-	-	-	-
Pretend to be/use title of solicitor (Other)	As above s. 92(1)(a)	0	1	1	2	0	-	-	-	-	-
Hold out/advertise as solicitor (Other)	As above s. 92(1)(b)	0	0	1	0	0	-	-	-	-	-
Practice as dentist-not registered (Other)	Dentists Act 1972 (Vic) s. 38(1)	0	3	1	0	4	2	4	-	-	-
False info/fraud registration as dentist (Other)	As above s. 44(1)	0	0	0	0	1	0	0	-	-	-
Practice chiropody-not registered	Chiropodists Act 1968 s. 14(3)	0	0	0	0	0	0	-	-	-	-
Unregistered doctor-carry out any act (Other)	Medical Practice Act 1994 (Vic) s. 62(1)(c)	-	0	0	0	2	0	0	0	0	0

** References are to the Victorian Crimes Act 1958 unless otherwise stated

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001	2001-2002	2002-2003
Unregistered doctor-take/use title (Other)	As above s. 62(1)(a)	-	3	5	0	0	0	0	0	0	0
Use title reg medical prac when not reg (Other)	As above	-	0	0	0	0	1	0	0	0	0
Practice as psychologist-Not registered (Other)	Psychological Practices Act 1965 (Vic) s. 39(1)	0	0	0	0	0	1	0	0	0	0
Advertise as psychologist-not registered (Other)	As above s. 29(1)	0	1	0	0	0	0	0	0	0	0
Use title/name of Psychologist (not registered)	As above s. 40(1)	0	0	0	0	0	0	0	0	0	4
Licences/books											
False info-Gaming lic/question/notice (Other)	Gaming Machine Control Act 1991 (Vic) s. 145(1)	0	0	1	1	0	0	0	0	0	0
LMCT Make false entry in dealings book (Other)	Motor Car Traders Act 1986 (Vic) s. 35(3)	0	0	0	0	0	2	8	0	0	0
LMCT Fail make entries in dealings book (other)	As above s. 35(2)	0	0	0	0	0	0	0	0	0	20
Remove any document from title office (Other)	Transfer of Land Act 1958 (Vic) s. 11(1)(f)	0	0	0	1	0	0	3	0	6	2
Conspiracy											
Conspire to defraud (Other)	Crimes Act 1914 (Cth) s. 86A	0	0	0	0	0	22	4	6	–	–
Collusive tendering (Other)	Collusive Practices Act 1965 (Vic) s. 3(1)(a)	0	0	0	0	0	0	1	0	–	–
Handling											
Obtain fin adv by deception (Handle stolen goods)+	s. 82(1)	N/A	N/A	N/A	2	123	284	170	162	194	235
Bring money to Vic – being proceeds of crime (Handle Stolen Goods)	Confiscation Act 1997 (Vic) s. 123(1)	-	-	-	-	-	10	9	2	2	0

cont...

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001	2001-2002	2002-2003
Postal											
Steal mail from any box/place (Theft (Other))	Crimes Act 1914 (Cth) s. 85K(1)(b)	0	1	1	5	17	4	1	1	0	0
Steal mail from post (Theft (Other))	As above s. 85K(1)(c)	0	6	1	0	1	4	78	3	1	0
Obtain drugs											
Obtain Restricted Substance - False Rep (Drugs (Possess/Use))	Drugs, Poisons And Controlled Substances Act 1981 (Vic) s. 36B(1)(a)	0	2	1	2	0	1	0	0	0	4
Obtain Drug by False Representation (Drugs (Possess/Use))	As above s. 36B(1)(a)	0	0	0	1	23	1	13	5	1	1
Harassment											
Stalk another person (Crimes Act) (Harassment)	s. 21A(1)	-	60	383	695	959	836	709	852	1037	1142
Use phone-telecommunications service-menace/harass/offend (Harassment)	Crimes Act 1914 (Cth) s. 85ZE	598	1461	1710	2537	2350	1157	11	1	758	247
Open/tamper with mail (C'wealth) (Harassment)	As above s. 85L(1) and 85V(1)	0	4	5	5	9	5	59	2	3	5
Cause mail to be wrongly delivered (Harassment)	As above s. 85N	0	1	0	2	0	0	0	0	0	1
Send postal message-forged signature (Other)	As above s.85T(a)	0	1	0	0	0	0	0	0	0	0

cont...

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001	2001-2002	2002-2003
Send postal message-sign fictitious name (Harassment)	As above s. 85T(b)	0	0	1	0	1	0	0	0	0	0
Cause phone carrier supply free service (Harassment)	As above s. 85ZF(b)	0	0	0	0	1	0	1	0	0	0
Defraud carrier of fee payable telecomm (Harassment)	As above s. 85ZF(a)	0	0	0	0	4	0	1	0	0	0
Defraud phone carrier of fee/charge (Harassment)	As above	0	2	0	102	4	0	0	0	0	0
Cause phone communication be misdirected (Harassment)	As above s. 85ZD	0	0	0	0	2	0	0	0	0	0
Tamper phone facility-hinder operation (Harassment)	As above s. 85ZG	0	0	1	1	42	36	26	5	15	0
Knowingly interfere with a facility (Harassment)	As above s. 85ZJ	0	0	0	0	14	177	132	17	73	15
Knowingly tamper with a facility (Harassment)	As above	0	0	0	0	0	32	7	1	2	0
Recklessly interfere with a facility (Harassment)	As above	0	0	0	0	0	3	3	0	0	2
Recklessly tamper with a facility (Harassment)	As above	0	0	0	0	1	7	2	0	0	0
Interfere/tamper with phone facility (Harassment)	As above	16	12	1	2	3	0	0	0	0	0

Notes to Appendix F

- *Source* Victoria Police *Statistical Review* 1993-2003
- A number of the *Crimes Act* 1914 (Cth) offences listed above (including ss. 29A, 85J, 85K, 85L, and 85ZF) were repealed with effect from 24 May 2001, by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act* 2000 (Cth).
- No entry in a cell (-) indicates that the offence did not exist at that time.
- (1) 2000-01: 3 (0 prev yr), No entry 1999-00, 1998-99: 71 (0 prev yr) and offence code here 321M not 321MQ
- Names in brackets after offence descriptions represent the Victoria police categorisation of the offences in the Statistical Reports.

+ N/A is given for this offence until 1996-97 because prior to that it did not appear in Victoria Police statistics separately under 'Handle Stolen Goods', only under 'Deception'. The rates recorded under the two headings of the offence are non-identical.

Appendix G: Financial Management Certification Checklist

This financial management certification checklist does not address the requirements for certification under the Tax Compliance Framework. The certification requirements under the Tax Compliance Framework are covered by a separate checklist and certification process.

In completing and signing the checklist, entities need to refer to the detailed compliance requirements contained in the Directions and mandatory procedures therein.

G *Denotes further on-line assistance is available via detailed guidance material.*

No	Direction Requirement	Direction Reference	Compliant	Partially Compliant	Non-Compliant	Not Applicable
Section 2 – Financial management Governance and Oversight						
Financial Code of Practice						
1	A 'Financial Code of Practice' exists covering areas required by the Directions, and is overseen by effective management with regards to its operation and handling of queries in respect of its compliance requirements.	2.1 G				
Financial Governance						
2	The Responsible Body is responsible for the governance and oversight of financial management and undertakes the duties with regards to: the review of external financial reports, setting of performance indicators, resourcing of an entity, procedures for effective and efficient budgeting, balance of authority, appointment of removal of the CFAO, risk management and financial internal controls, major capital expenditures, acquisitions or divestitures, economic and effective and efficient allocation of public funds, and meets often enough to undertake an effective financial governance role.	2.2 G				
3	The Accountable Officer and the CFAO have, within the last 12 months, made formal statements to the Responsible Body/Board that the entity's financial report presents a true and fair view and on risk management, internal compliance and control systems.	2.2 G				

No	Direction Requirement	Direction Reference	Compliant	Partially Compliant	Non-Compliant	Not Applicable
4	An Audit Committee has been constituted and has a membership that is consistent with the criteria specified in Direction 2.2. The Audit Committee has functioned within the parameters of a Charter, which has been approved by the Responsible Body and provided to each member of the Audit Committee. *Where an Audit Committee does not exist, a written exemption must be obtained from the Minister for Finance and the Responsible Body undertakes the functions of an Audit Committee. (If your entity is eligible for an exemption and has obtained one you should tick – compliant, if you have not obtained an exemption at the time of certification you should tick - non-compliant with an appropriate comment)*	2.2 G				
5	The Audit Committee has had direct access to: • Internal and external auditors • The Accountable Officer • The CFAO • The Public Sector Agency's management (through the Accountable Officer)	2.2 G				
Financial Risk Management						
6	The Public Sector Agency has a financial risk management policy and internal control system in place which addresses the risks associated with the financial management of the Public Sector Agency.	2.3 G				
7	The financial risk profile has been critically reviewed by the Responsible Body within the last 12 months.	2.3 G				
Delegations of Authority						
8	The Responsible Body has adopted Delegations of Authority which conform to the requirements of the Directions and these Delegations have been reviewed by the Responsible Body within the last 12 months.	2.4				
Internal Audit						
9	An internal audit function exists and works within the parameters of a Charter and an internal audit plan, both of which have been approved by the Audit Committee and are consistent with the requirements of the Directions. *Where an Internal Audit function does not exist, a written exemption must be obtained from the Minister for Finance. (If your entity is eligible for an exemption and has obtained one you should tick – compliant, if you have not obtained an exemption at the time of certification you should tick - non-compliant with an appropriate comment)*	2.5 G				

No	Direction Requirement	Direction Reference	Compliant	Partially Compliant	Non-Compliant	Not Applicable
External Audit						
10	The Audit Committee has taken the actions required by Direction 2.6 in respect of external audit for the financial year (or part thereof) just ended, including inviting the external auditor to all relevant meetings and making time available to meet privately to discuss audit related issues at least once within the last 12 months.	2.6				
Section 3 – Financial Management Structure, Systems, Policies and Procedures						
Public Sector Agency Financial Management Team Structure						
11	Roles and responsibilities for positions within the financial management team structure, and the prerequisite skills, qualifications and experience have been defined and documented.	3.1.1 G				
Chief Finance and Accounting Officer (CFAO)						
12	The prerequisite skills, qualifications and experience for the CFAO are clearly defined and documented together with position description, role, duties, rights and responsibilities.	3.1.2 G				
13	The CFAO has endorsed financial information submitted to the Accountable Officer, Responsible Body and/or other senior executive forums within the Public Sector Agency.	3.1.2 G				
Policies and Procedures						
14	There are documented and communicated policies and procedures covering the requirements of the Directions in respect of financial administration and management and these have been ratified by the Responsible Body.	3.1.3 G				
Chart of Accounts						
15	The CFAO or their delegate has established, maintained and distributed a Chart of Accounts, which meets the requirements of the Directions.	3.1.4 G				
Managing Outsourced Services						
16	All outsourced finance functions or services are governed by contracts, service level agreements or other documented arrangements, each of which has been reviewed for compliance in the past twelve months.	3.1.5 G				
17	All finance functions or services outsourced during the financial year (period) just ended were subjected to a cost-benefit analysis, approved by the Responsible Body, and detailed in the form of a contract, service level agreement or equivalent which allows for internal and external audit scrutiny.	3.1.5 G				

No	Direction Requirement	Direction Reference	Compliant	Partially Compliant	Non-Compliant	Not Applicable
	Information Technology Management					
18	The Accountable Officer has reviewed the use of Information Technology used for financial management within the last 12 months to assess information technology risks and their impact on financial management.	3.2.1 G				
	Information Technology Operations					
19	There are documented and tested back up, disaster recovery and business continuity procedures in place that are commensurate with the Public Sector Agency's financial management needs.	3.2.2 G				
20	A formal assessment has been undertaken within the last 12 months of whether financial management information that is sensitive to the Public Sector Agency and stakeholders is adequately controlled and secured.	3.2.1 3.2.2 3.2.3 G				
	Development					
21	A business case was prepared and approved by the IT Steering Committee or Responsible Body and a formal IT development methodology was adopted, for the development of any financial management systems and technology during the year.	3.2.4 G				
	Change Control					
22	A change control process was followed for changes made to financial management systems.	3.2.5 G				
	Education and Training					
23	The training and education needs for the financial management team have been reviewed by the CFAO or their delegated authority within the last 12 months, and an appropriate program developed to address the training and education needs of financial management staff.	3.3 G				
	Policies and Procedures					
24	Policies and procedures have been developed, documented and approved for the following financial cycles or activities, and to satisfy the requirements of the Directions and the *Financial Management Act* 1994*:* • Revenue • Cash Handling • Bank Accounts • Cash Flow Forecasting • Procurement • Expenditure • Employee Costs • Commission on Payroll Deductions • Physical and Intangible Assets • Liabilities • Reconciliations • Administration of Discretionary Financial Benefits	3.4 G				

No	Direction Requirement	Direction Reference	Compliant	Partially Compliant	Non-Compliant	Not Applicable
Section 4 – Financial Management Reporting						
Internal Financial Management Reporting						
25	Requirements for internal financial management reports have been identified and relevant reports have been produced at regular intervals throughout the financial year.	4.1 G				
26	Financial management reports have been tabled and discussed by the Responsible Body or another recognised senior forum as determined by the Responsible Body, and reports tabled at these forums have been reviewed by the CFAO or delegate, prior to being tabled.	4.1 G				
Reporting Requirements in terms of Part 7 of the FMA						
27	The Financial Statements and Report of Operations have been prepared in accordance with Part 7 of the *Financial Management Act* 1994 and in the required timeframes.	4.2				
Other External Reporting						
28	All external reporting requirements have been identified and relevant reports delivered completely, accurately and in a timely manner following review by the CFAO or their delegate.	4.3				
Financial Performance Management and Evaluation						
29	The Responsible Body has developed financial key performance indicators (KPIs) working with management, and there is monitoring and reporting of performance against these to the Responsible Body and/or the Accountable Officer.	4.4 G				

Source: Department of Treasury and Finance, Victoria, 2003, *Whole of Government Financial Management Compliance Framework: Explanatory Framework Document*, Department of Treasury and Finance, Melbourne.

Appendix H: Recommendations

Recommendation 1a

The Committee recommends that the Attorney-General for the State of Victoria seek a review of the Australian Standard Offence Classification, to enable more specific information on fraud and electronic commerce-related offences to be identified (p.61).

Recommendation 1b

The Committee recommends that the Attorney-General for the State of Victoria also request the Australian Bureau of Statistics to include fraud and other deception offences in its regular surveys of household and personal victimisation (p.61).

Recommendation 1c

The Committee recommends that any changes made to the Australian Standard Offence Classification be reflected in statistics that are collected and published by police, courts and correctional agencies in Victoria (p.61).

Recommendation 2a

The Committee recommends that legislation governing professional regulatory bodies, such as the Medical Practitioners Board of Victoria and the Legal Practice Board, be amended to require the annual publication of specific information about fraud and dishonesty-related complaints that have been referred for investigation, how those complaints were dealt with and the outcomes of investigations (p.64).

Recommendation 2b

The Committee recommends that all professional regulatory agencies be required to notify VFIRC of all matters involving fraud and financial crime or professional misconduct of a financial nature that come to their attention (p.64).

Recommendation 3a

The Committee recommends the establishment of a Victorian Fraud Information and Reporting Centre (VFIRC), within Victoria Police, as a dedicated agency staffed by unsworn analysts, to:

i collect and disseminate information about the nature and extent of fraud occurring across Victoria;

ii collect and publish statistics on fraud; and

iii receive complaints of fraud from members of the public and public and private sector organisations for referral to appropriate agencies for investigation (p.88).

Recommendation 3b

The Committee recommends that VFIRC would not have an operational policing function in the investigation of cases of fraud. It should not be located within the Major Fraud Investigation Division of Victoria Police (p.88).

Recommendation 3c

The Committee recommends that VFIRC should be responsible for the collection and publication of statistics in relation to the nature and extent of fraud in Victoria, including information on prosecution and sentencing of fraud offenders (p.88).

Recommendation 3d

The Committee recommends that VFIRC should play a central role in relation to the reporting of fraud. All reports of fraud and financial crime in Victoria should be received by VFIRC either by direct notification from members of the public or as notified by other agencies (p.88).

Recommendation 3e

The Committee recommends that VFIRC should be located centrally in dedicated premises in order to facilitate access and to enhance visibility (p.88).

Recommendation 3f

The Committee recommends that VFIRC should receive a dedicated budget administered by Victoria Police (p.88).

Recommendation 3g

The Committee recommends that VFIRC should be the central Victorian agency responsible for the collection and analysis of reports of fraud perpetrated against public sector agencies in Victoria and by Victorian public servants. Individual government agencies in Victoria should be required to notify VFIRC of all cases involving suspected fraud that are required to be reported to the Minister for Finance. VFIRC analysts would then compile reports for the Minister for Finance as required under the *Financial Management Act 1994* (Vic.) (p.88).

Recommendation 4a

The Committee recommends the establishment of an Australian Fraud Centre (AFC), to collect and disseminate information about the nature and extent of fraud occurring across Australia and to help co-ordinate a national response to fraud. In order to facilitate the establishment of the AFC, the Attorney-General for the State of Victoria should propose its establishment at the next meeting of the Standing Committee of Attorneys-General (p.90).

Recommendation 4b

The Committee recommends that the AFC should be involved in the collection and dissemination of fraud intelligence and the publication of national fraud statistics (p.90).

Recommendation 4c

The Committee recommends that the AFC should be housed within the infrastructure of either the Australian Crime Commission or the Australian Federal Police (p.90).

Recommendation 5a

The Committee recommends that surveys be conducted of businesses and companies operating in Victoria to determine the nature and extent of their fraud and electronic commerce-related victimisation (p.91).

Recommendation 5b

The Committee recommends that a study be undertaken in Victoria to determine the financial and indirect costs associated with fraud and electronic commerce-related crime in Victoria (p.91).

Recommendation 5c

The Committee recommends that research be undertaken to determine the nature, extent and financial cost of fraud perpetrated in the higher education sector in Victoria (including Tertiary and Further Education Institutes), and steps which can be taken to address this problem (p.91).

Recommendation 5d

The Committee recommends that research be undertaken to ascertain the links between fraud and gambling, and ways in which this issue can be addressed (p.91).

Recommendation 6a

The Committee recommends that a requirement that all public sector entities (including local government) implement and maintain a fraud control policy be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standard AS8001-2003 *Fraud and Corruption Control* and the New South Wales Audit Office's *Fraud Control: Developing an Effective Strategy,* and should include elements relating to the prevention, detection, reporting and investigation of fraud, as well as containing a fraud response plan. It should also specifically address the risks of fraud arising out of the use of electronic commerce (p.139).

Recommendation 6b

The Committee recommends that all public sector entities be required to certify their compliance with the relevant fraud control direction in the annual certification process established by the Financial Management Compliance Framework (p.140).

Recommendation 7a

The Committee recommends that VFIRC promote the implementation of fraud control policies by businesses and corporations in the private sector, using Standard AS8001-2003 *Fraud and Corruption Control* as a model. VFIRC should provide assistance to such organisations in drafting and implementing such policies if necessary (p.141).

Recommendation 7b

The Committee encourages the development of a fraud control certification service for the private sector, to certify compliance with Standard AS8001-2003 *Fraud and Corruption Control*. If such a service is established, its existence should be promoted by VFIRC and certification encouraged. A list of those organisations that have had their policy certified should be published on VFIRC's web site (p.141).

Recommendation 8

The Committee recommends that appropriate sanctions be introduced for failure to comply with the Code of Conduct for the Victorian Public Sector (p.144).

Recommendation 9a

The Committee recommends that an Internet industry body be established in Victoria. Steps should be taken to facilitate the establishment of such a body, including the provision of seed funding if necessary. Any body that is established should be encouraged to develop a Victorian Internet Industry Code of Conduct which deals with fraudulent content and unsolicited material transmitted electronically (p.148).

Recommendation 9b

The Committee recommends the promotion and use across Victoria of the Department of Treasury's *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business*, as well as the Internet Industry Association's *Cybercrime Code* when finalised (p.148).

Recommendation 10

The Committee recommends that industry Codes of Conduct relating to electronic commerce, the Internet and online gambling be mandated under Part IVB of the *Trade Practices Act 1974* (Cth) (p.150).

Recommendation 11a

The Committee recommends that all public sector entities (including local government) be required to implement and maintain an information security management policy and that this requirement be included in the Standing Directions of the Minister for Finance. The content of the policy should be based on Standards AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management;* AS/NZS 7799.2:2003 *Information security management – Part 2: Specification for information security management systems*; and HB 231:2000 *Information security risk management guidelines* (p.156).

Recommendation 11b

The Committee recommends that all public sector entities (including local government) be required to certify their compliance with the relevant Information Security Management Direction in the annual certification process established by the Financial Management Compliance Framework (p.156).

Recommendation 12a

The Committee recommends that VFIRC promote the implementation of information security management strategies by businesses and corporations in the private sector, using the Standards Australia Information Security Management Standards as a model (p.156).

Recommendation 12b

The Committee recommends that VFIRC should also encourage businesses and corporations in the private sector to have their information security management systems certified as being in compliance with the Standards Australia Information Security Management Standards. A list of those organisations that have had their systems certified should be published on VFIRC's web site (p.156).

Recommendation 13

The Committee recommends that all financial institutions operating in Australia encrypt all data moving to and from EFTPOS and ATM terminals (p.156).

Recommendation 14

The Committee recommends that individual identification cards should not be introduced at a national or state level in Australia (p.164).

Recommendation 15a

The Committee recommends that a national approach be taken to the verification of documents used to establish identity, and encourages the Victorian government to co-operate fully with Australian government initiatives designed to enable the online verification of evidence of identity information and to improve the '100-point system' established under the *Financial Transaction Reports Regulations 1990* (Cth) (p.166).

Recommendation 15b

The Committee recommends that public sector agencies and private sector organisations which issue documents that can be used as evidence of identity (such as birth certificates and driver's licenses) take steps to cleanse their databases of information to ensure that information is accurate and current, and that they co-operate with the development of online verification systems (p.166).

Recommendation 16a

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to ensure that effective security measures are used in those documents to minimise the risk of documents being altered or counterfeited (p.169).

Recommendation 16b

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity be required to comply with high level standards with respect to the security of materials used for the creation of such documents (including blank paper, inks, and plastic cards and their components), and that issuing branch offices be required to adopt uniform security standards (p.169).

Recommendation 16c

The Committee recommends that Victorian agencies which issue documents that can be used as evidence of identity take steps to minimise the extent to which documents are sent to clients by ordinary mail, and that alternative procedures be developed to minimise loss and misappropriation of documents in transit (p.169).

Recommendation 17

The Committee recommends that biometric systems not be widely implemented by the Victorian Public Service for fraud control purposes until the technology is more accurate and reliable, appropriate standards have been developed, and biometric-specific privacy protections have been incorporated into legislation (p.177).

Recommendation 18

The Committee recommends that the Victorian government should support the early roll-out of EMV standard computer-chip plastic cards for use in electronic transactions in conjunction with Personal Identification Number (PIN) authentication (p.179).

Recommendation 19a

The Committee recommends the adoption of the proposals set out in the *Gatekeeper Strategy* concerning secure electronic transactions, and supports the adoption of the *Gatekeeper*-compliant framework at a state level (p.182).

Recommendation 19b

The Committee recommends that Registration Authorities which issue public-private key pairs for use in secure electronic transactions be required to adopt the same standards for identification of users as are required to open an account with a financial institution under the Financial Transaction Reports Regulations 1990 (Cth) (p.182).

Recommendation 19c

The Committee recommends that legislation be passed making it illegal to generate and retain a copy of a private key without consent, once the original has been passed on (p.182).

Recommendation 20

The Committee recommends that VFIRC should promote the use in the public and private sectors of effective measures to screen personnel prior to employment, to assist in the detection of individuals who might be at risk of behaving dishonestly (p.185).

Recommendation 21a

The Committee recommends that VFIRC establish and maintain a system for the accreditation of web seals that comply with accepted standards concerning content and honesty, and that this system be promoted for use by all Victorian online trading organisations (p.188).

Recommendation 21b

The Committee recommends that consideration be given to creating a criminal offence for an individual or corporation to apply a web seal to an Internet site without appropriate authorisation from the accrediting agency (p.188).

Recommendation 22a

The Committee recommends that VFIRC be the central Victorian agency responsible for providing information to the public and private sectors in relation to fraud prevention matters (p.196).

Recommendation 22b

The Committee recommends that, in addition to the activities outlined in the recommendations above, VFIRC conduct the following fraud prevention activities:

i. Carry out programs designed to inform the business community and individuals in Victoria of the risks of fraud and electronic commerce-related crime and of the fraud prevention measures that can be used to minimise the risk of victimisation. This should include a mail-out to all Victorian households of an information brochure on prevention methods that could be used to reduce the risk of fraud victimisation in consumer transactions, business transactions, and electronic transactions, highlighting the importance of the responsible maintenance of passwords and PINs;

ii. Conduct training sessions and/or seminars in relation to fraud control (including information security management), as well as encouraging public and private sector agencies to disseminate and explain their fraud control policies widely amongst staff and periodically hold in-house fraud prevention training. In particular, where staff are required to verify documents used to establish identity, organisations should be encouraged to train them in identifying counterfeit and altered documents;

iii. Develop best practice guidelines to help organisations implement authentication systems (including password management systems) appropriate to their security needs; and

iv. Develop a web site containing fraud prevention information for the public and private sectors and for individuals (p.196).

Recommendation 23

The Committee recommends an informal fraud prevention and control network, such as the New South Wales Corruption Prevention Network, be established in Victoria. Steps should be taken to facilitate the establishment of such a network, including the provision of seed funding if necessary. The existence of the network should be promoted by VFIRC (p.199).

Recommendation 24a

The Committee supports the permanent establishment of various registers concerning identity-related fraud, to be administered either by the Australian Crime Commission or the Australian Federal Police. They would include a register of fraudulent identities and associated fraudulent documents, a victims of identity fraud register, a stolen/lost document register and a document image register (p.201).

Recommendation 24b

The Committee recommends that in order to facilitate the establishment of these registers, the Attorney-General for the State of Victoria propose their establishment at the next meeting of the Standing Committee of Attorneys-General (p.201).

Recommendation 25a

The Committee recommends that the Australian Securities and Investments Commission be notified of all people disqualified from managing corporations due to dishonesty-related convictions, for inclusion in the Disqualified Persons Register (p.204).

Recommendation 25b

The Committee recommends a similar registration system be introduced in Victoria within the Office of Consumer and Business Affairs, in which people can be disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations if they have been convicted of an offence that involves dishonesty and is punishable by imprisonment for at least three months (p.204).

Recommendation 25c

The Committee recommends that the Office of Consumer and Business Affairs Victoria be notified of any people who have been disqualified from being business proprietors or office bearers, members of the committee of management or public officers of incorporated associations due to dishonesty-related convictions, for inclusion in a Victorian Disqualified Persons Register which it develops and maintains (p.204).

Recommendation 25d

The Committee recommends that all Victorian professional regulatory agencies, such as the Legal Practice Board and the Medical Practitioners Board of Victoria, be required to notify VFIRC when one of their members has been deregistered due to fraud or dishonesty-related conduct, for inclusion in a register to be maintained by VFIRC. Each professional association should also be required to maintain its own registers of those who have been deregistered due to fraud or other dishonesty-related offences (p.204).

Recommendation 25e

The Committee recommends that information on VFIRC's register be made available to persons seeking it for legitimate reasons and that the disclosure of information by VFIRC be carried out in accordance with privacy principles (p.204).

Recommendation 26a

The Committee recommends that the procedures associated with the identification of persons who seek to register a business or incorporated association in Victoria be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of business proprietors or individuals who register an incorporated association (p.206).

Recommendation 26b

The Committee recommends that the *Business Names Act 1962* (Vic) be amended to require the Commissioner of Consumer Affairs not to register business names closely similar to existing names and likely to be confused with or mistaken for each other (p.206).

Recommendation 27a

The Committee recommends that the Attorney-General for the State of Victoria correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the identification of persons who seek to incorporate a company, to require them to provide the same evidence of identity of the person seeking incorporation as is necessary to open an account with a financial institution. The correspondence should also include a request that procedures be put in place to assist in detecting the use of false information concerning the names of directors and office bearers of companies (p.206).

Recommendation 27b

The Committee recommends that the Attorney-General for the State of Victoria also correspond with the Commonwealth Attorney-General seeking an amendment to the procedures associated with the choice of company names, so that company names closely similar to existing names and likely to be confused with or mistaken for each other not be registered (p.206).

Recommendation 28a

The Committee recommends that the procedures associated with the identification of persons who seek to register Internet domain names be altered to require the same evidence of the identity of the person seeking registration as is necessary to open an account with a financial institution. Procedures should also be put in place to assist in detecting the use of false information in relation to the names of registrants of domain names (p.206).

Recommendation 28b

The Committee recommends that the system of registering Internet domain names be reformed to prevent the registration of misleading domain names (p.206).

Recommendation 29

The Committee recommends that prior to employers monitoring their employees' use of the Internet, employees must be informed that they may be monitored, and be advised of the extent to which they can use computers for their own purposes (p.212).

Recommendation 30

The Committee recommends that a system of unique identification numbers should not be introduced at a national or state level (p.214).

Recommendation 31

The Committee recommends that the *Whistleblowers Protection Act 2001* (Vic) be extended to individuals who report suspected fraud and offences involving dishonesty committed in the private sector (p.220).

Recommendation 32

The Committee recommends that VFIRC establish a hotline for reporting public or private sector fraud. It should be possible for people to report anonymously if desired. VFIRC should determine whether further investigation is required, and if so which is the most appropriate body to carry out that investigation. When providing the appropriate body with the information necessary to conduct such an investigation, care must be taken to protect the whistleblower, in accordance with the procedures set out in the *Whistleblowers Protection Act 2001* (Vic) (p.220).

Recommendation 33

The Committee recommends that the question of whether and how individuals should be compensated for reporting instances of suspected fraud should be referred to the Victorian Law Reform Commission for further inquiry. Issues to be addressed by the inquiry should include whether a fund should be established to compensate individuals who have suffered loss as a result of reporting fraud, the desirability of introducing *qui tam* laws in relation to whistleblowers, and whether scales of costs applicable to witnesses in fraud cases should be reviewed (p.220).

Recommendation 34a

The Committee recommends that VFIRC be the central Victorian agency to receive all reports of fraud from individuals, public sector agencies and private sector organisations (p.231).

Recommendation 34b

The Committee recommends that all public sector agencies and private sector organisations that become aware of incidents of fraud be required to notify VFIRC within 10 working days. The Committee recommends that failure to comply with this requirement be subject to appropriate sanctions (p.231).

Recommendation 34c

The Committee recommends that all public sector agencies and private sector organisations be required to notify VFIRC of the outcome of any fraud-related investigations and prosecutions within 10 working days of the outcome being known or a decision being made (p.231).

Recommendation 34d

The Committee recommends that a criminal offence be created of failure to report a serious offence involving dishonesty (being an offence within the Australian Standard Offence Classification category of dishonesty) where the victim believes that any financial loss suffered would amount to at least $100,000 (p.231).

Recommendation 34e

The Committee recommends that VFIRC act as a clearinghouse, determining which is the appropriate agency (if any) to act upon the report, and providing that agency with the report. Relevant agencies would include professional regulatory bodies such as the Legal Practice Board or the Medical Practitioners Board of Victoria, Commonwealth agencies such as the Australian Crime Commission or the Australian High Tech Crime Centre, and state agencies such as the Office of the Auditor-General or Victoria Police. VFIRC should not have any investigatory powers (p.231).

Recommendation 34f

The Committee recommends that all reports received by VFIRC be forwarded to Victoria Police. VFIRC should have the power to recommend which branch of Victoria Police (such as the Major Fraud Investigation Division or a Criminal Investigation Unit) would be most appropriate to handle the matter and to recommend that Victoria Police act in partnership with another public or private sector body, including the victim. Where the victim makes such a request, VFIRC should also be able to recommend that no police action be taken at all. Victoria Police would, however, retain final discretion in deciding how to proceed with any matter (p.231).

Recommendation 34g

The Committee recommends that VFIRC organise a forum with representatives from all appropriate agencies, to help devise guidelines for determining which agency is best placed to investigate reports that have been received (p.232).

Recommendation 34h

The Committee recommends that VFIRC produce a best practice guide to reporting fraud, including a description of what information should be provided. The guide should contain specific information on preparing reports where the matter is likely to require further police action to be taken. Similar information should be published on the VFIRC web site (p.232).

Recommendation 35

The Committee recommends that the requirement under Direction 4.3 of the Standing Directions of the Minister for Finance, requiring cases of suspected or actual theft, irregularity or fraud under the control of their departments to be notified to the relevant Minister and the Auditor-General, be extended to all public sector agencies in Victoria including local government departments. The Auditor-General's resources should be increased to deal with any increased caseload (p.232).

Recommendation 36

The Committee supports the attempt by the Australian Institute of Professional Investigators (Victorian Chapter) and the Victoria Police Major Fraud Investigation Division to draft a set of policy standards to form the basis for a national framework for all fraud investigation (p.235).

Recommendation 37

The Committee recommends that VFIRC promote the importance of private sector organisations specifying in their fraud control policies the steps to be taken in investigating suspected fraud (p.238).

Recommendation 38

The Committee recommends that public and private sector fraud control policies and investigations follow the procedures set out in the Standards Australia *Guidelines for the management of IT evidence*, to ensure that electronic evidence is preserved (p.238).

Recommendation 39a

The Committee recommends that primary responsibility for the investigation of fraud in Victoria remain with Victoria Police (p.250).

Recommendation 39b

The Committee recommends that additional resources be provided to Victoria Police to enable it to:

i. provide additional fraud-related training to its members;

ii. retain personnel with particular experience in fraud;

iii. purchase new technologies necessary to combat high tech crime;

iv. establish a new sub-division to deal with complex financial crimes that involve small-value losses which do not fall within the scope of the Major Fraud Investigation Division but are also unable to be handled by Criminal Intelligence Units owing to their complexity or the nature of the investigatory expertise required; and

v. develop clear guidelines to determine when matters will be examined by the new sub-division, the Major Fraud Investigation Division, Criminal Intelligence Units, or any other parts of Victoria Police, and when Victoria Police should work in conjunction with other state or national agencies or other bodies (p.250).

Recommendation 39c

The Committee recommends that a Ministerial Task Force be established to examine the policing of fraud, with a particular focus on the issue of partnership policing, namely the development of procedures that can assist law enforcement agencies to work together with the public and private sectors to build an effective fraud response framework (p.250).

Recommendation 40a

The Committee recommends that an inquiry be conducted into the introduction of a statutory system for the professional regulation and registration of accountants, financial advisers and other financial consultants (such as mortgage brokers) who practise in Victoria, with a view to determining standards for admission to practise, and procedures for restriction of registration on proof of professional misconduct. The Committee recommends that legislation governing other statutorily recognised professions in Victoria be used as a model (p.258).

Recommendation 40b

The Committee recommends that action be taken by the Australian Securities and Investments Commission to ensure that individuals who are prohibited from practising in the financial services industry are unable to circumvent such action by continuing to practise in other advisory roles (p.258).

Recommendation 41

The Committee supports continuing attempts to harmonise nationally the law relating to fraud and other dishonest conduct, including crimes involving misuse of identity and dishonest practices relating to payment cards and electronic payment systems (p.265).

Recommendation 42

The Committee recommends that the *Crimes Act 1958* (Vic) be amended to reflect the recommendations of the Model Criminal Code Officers Committee in relation to dishonesty offences, including fraud and forgery, as enacted in Divisions 133-137 and 143-145 of the *Criminal Code Act 1995* (Cth). In amending the law, it should be ensured that:

i the means of proving dishonesty in Victoria be determined according to the standards of ordinary people, and known by the accused to be dishonest according to those standards;

ii. the definition of 'property' that can be fraudulently obtained includes intellectual property and computer data;

iii. company directors and employees can be charged with the relevant offences where they have defrauded their own company;

iv. people can be charged with the relevant offences where they have defrauded a pooled fund;

v. offences are applicable to fraud committed in an online environment; and

vi. Victorian fraud and dishonesty-related offences be able to be charged in any case where the offence was committed in Victoria, or where the victim was in Victoria at the relevant time (p.265).

Recommendation 43

The Committee recommends that a general fraud offence should not be established in Victoria (p.265).

Recommendation 44a

The Committee recommends that the development of a national legislative response to questions of theft of identity, identity-related fraud and credit card fraud including card skimming and the possession of equipment or devices used in connection with credit card fraud be referred to the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General for investigation and report. In doing so, consideration should be given to:

i. The introduction of an offence of assuming a false identity with the intention to commit a serious offence;

ii The introduction of offences proscribing the possession of equipment or devices (including plastic cards), with intent to dishonestly counterfeit or alter documents or to assist in the commission of an offence involving dishonesty;

iii. The introduction of offences proscribing the importation, possession and use of equipment or devices (including plastic cards), with intent to dishonestly obtain funds through the deception or manipulation of payment systems; and

iv Reversing the onus of proof (p.273).

Recommendation 44b

The Committee recommends that criminal offences relating to theft of identity, identity-related fraud or credit card fraud should not be implemented until a national approach to these issues has been agreed upon (p.273).

Recommendation 44c

The Committee recommends that any new criminal offences relating to theft of identity, identity-related fraud or credit card fraud should be technology-neutral (p.273).

Recommendation 45

The Committee supports national initiatives designed to reduce the incidence of unsolicited email ('spam') (p.280).

Recommendation 46

The Committee recommends that the issue of whether Victorian courts should be given the power to freeze property at the request of a foreign state while forfeiture proceedings take place in their jurisdiction be further investigated (p.283).

Recommendation 47

The Committee recommends that juries continue to be the appropriate body to make factual determinations in cases involving fraud and dishonesty-related offences. The Committee does not support the introduction of specialist juries, panels of assessors or trial by judge alone (p.291).

Recommendation 48

The Committee recommends that there should be specialist fraud lists in the Supreme and County Courts (p.291).

Recommendation 49

The Committee recommends that additional funding be allocated to the improvement of courtrooms in Victoria to enable information to be provided to judges, lawyers and members of juries electronically through the use of computers and displayed on screens in courtrooms during proceedings (p.291).

Recommendation 50

The Committee recommends that maximum penalties for fraud and deception-related offences be consistent with those set out in the *Criminal Code Act 1995* (Cth) (p.298).

Recommendation 51a

The Committee recommends that VFIRC be the central agency within Victoria responsible for co-ordinating support services for victims of fraud-related offences and their families, including victims of identity theft (p.299).

Recommendation 51b

The Committee recommends that procedures be developed to assist victims of identity theft to recover any loss or damage sustained as a result of the theft, including restoration of their credit rating. Consideration should be given to:

i. the development of a formal certificate (with appropriate security) outlining the name of the victim and the offence, which could be used to prove that they have been the victim of a crime; and

ii. the development of a standard affidavit for victims of identity crimes to be used by victims trying to counter the effects of identity theft, alleviating the need for filling out multiple forms (p.299).

Recommendation 51c

The Committee recommends that VFIRC provide information to victims of identity theft, including steps that can be taken to recover any loss or damage sustained as a result of the theft (p.299).

Bibliography

The Age 2000, 'IT 1 News', 11 July, p.2.

American Association of Retired Persons 1996, *Telemarketing Fraud and Older Americans: An AARP Study*, Princeton Survey Research Associates, Princeton.

American Institute of Certified Professional Accountants 2000, *CPA Webtrust.* http://www.cpawebtrust.org/.

Arnold, T. 2002, 'An electronic citadel: A method for securing credit card and private consumer data in e-business sites and database systems', *Journal of Economic Crime Management*, vol. 1, no. 1, Summer. Also at, http://www.jecm. org/02_vol1_ issue1_art4.pdf.

Association of Certified Fraud Examiners 2002, *2002 Report to the Nation: Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, Austin, Texas.

Association for Payment Clearing Services 2003, *Card Fraud: The Facts 2003*, Association for Payment Clearing Services, London.

Atkinson, The Hon. M. J. 2003, 'Criminal Law Consolidation (Identity Theft) Amendment Bill: First Reading', *Parliamentary Debates, South Australia, House of Assembly*, 15 October. http://www.parliament.sa.gov.au/catalog/ hansard/2003/ha/ wh151003.ha.htm.

Attorney-General's Department, Australia 1999, *Contributions to Electronic Commerce: What Law Enforcement and Revenue Agencies Can Do*, Report of the Action Group into the Law Enforcement Implications of Electronic Commerce, Australian Government Publishing Service, Canberra.

.au Domain Administration Limited 2001, 'auDA today issued the following consumer alert; WARNING-.com.au Domain Name Licence Renewals Be Wary of Renewal Notices'. At, http://www.auda.org.au/alert_renewal.html.

Auditing and Assurance Standards Board 2002, *Australian Auditing Standard AUS 210: The Auditor's Responsibility to Consider Fraud and Error in an Audit of a Financial Report*, Auditing and Assurance Standards Board.

Australasian Centre for Policing Research 2000, *The Virtual Horizon:Meeting the Law Enforcement Challenges – Developing an Australasian Law Enforcement Strategy for Dealing With Electronic Crime*, A scoping paper, Police Commissioners' Conference Electronic Crime Working Party, Australasian Centre for Policing Research. Also at, http://www.acpr.gov.au/publications2.asp ?Report_ID=102.

Australasian Centre for Policing Research 2001, *Electronic Crime Strategy of the Police Commissioners' Conference Electronic Crime Steering Committee 2001 – 2003*, March. Also at, http://www.a cpr.gov.au/publications2.asp?Report_ID=103.

Australian Associated Press (AAP) 2002a, 'Alleged CityLink conman heads west, fearing jail – Court', *f2 Network News*, 3 July. At, http://news.f2.com.au/2002/07/03/FFX62RT363D.html.

Australian Associated Press (AAP) 2002b, 'Man faces court over CityLink credit theft', *NineMSN News*, 8 August, http://news.ninemsn.com.au/National/ story_ 36996.asp.

Australian Associated Press (AAP) 2003, 'ATM skimmer gets three years' jail', http://news.ninemsn.com.au/National/story_52772.asp

Australian Associated Press (AAP) 2003a, 'Insider trading sends Rivkin inside for weekends only', *The Age*, 30 May, p.5.

Australian Broadcasting Authority (ABA) 2002, *Annual Report 2001–2002*, http://www.aba.gov.au/abanews/annRpt/an01-02/index.htm.

Australian Bureau of Statistics 1996a, *Census of Population and Housing: Selected Family and Labour Force Characteristics for Statistical Local Areas* (Cat. Nos. 2017.0-8), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1996b, *Prisoners in Australia 1994: Results of the 1994 National Prison Census*, Australian Government Publishing Service, Canberra.

Australian Bureau of Statistics 1997a, *Australian Standard Classification of Occupations*, Second Edition and ASCO Coder, ABS No. 1220.0.30.001, Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1997b, *National Correctional Statistics: Prisons*, Australian Government Publishing Service, Canberra.

Australian Bureau of Statistics 1997c, *1995 National Health Survey: Summary of Results* (Cat. No. 4364.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1997d, *Prisoners in Australia 1995: Results of the 1995 National Prison Census*, National Corrective Services Statistics Unit, Australian Bureau of Statistics, Melbourne.

Australian Bureau of Statistics 1998a, *Household Use of Information Technology, Australia* (Cat No 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1998b, *Use of the Internet by Householders, Australia* (Cat No 8147.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1999, *Household Use of Information Technology, Australia* (Cat No 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2002a, *Australian Economic Indicators*, (1350.0), October 2002, Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2002b, *Internet Activity*, (8153.0) March Quarter 2002, Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2002c, *Household Use of Information Technology, Australia* (Cat No 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2003a, *Australian Economic Indicators*, (1350.0), October 2003, Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2003b, *Internet Activity*, (8153.0) March Quarter 2003, Australian Bureau of Statistics, Canberra.

Australian Capital Territory (ACT) Government 1994, *Fraud and Corruption Control in the ACT Government Service*, Fraud Prevention Unit, Department of Public Administration, Canberra.

Australian Commission for the Future 1996, *Smart Cards and the Future of Your Money*, Australian Commission for the Future, Melbourne.

Australian Competition and Consumer Commission (ACCC) 1997, *International Internet Sweep Day 1997*. At, http://www.accc.gov.au/ecom2/Inter_net_Sweep_97.htm.

Australian Competition and Consumer Commission (ACCC) 1999, 'Court finds the Australasian Institute misled students', *Media release*, 22 December. At, http://www.accc.gov.au/media/mr1999/mr%2D251%2D99.htm. (See also http://www.accc.gov.au/pubreg/87B_PG2.htm).

Australian Competition and Consumer Commission (ACCC) 2001, *International Internet Sweep Days*. At, http://www.accc.gov.au/ecom2/Inter_net_Sweep.htm.

Australian Competition and Consumer Commission (ACCC) 2002a, 'Global enforcement action brings "sweep"ing change', *Media release*, 23 September. At, http://203.6.251.7/accc.internet/digest/view_media.cfm?RecordID=806.

Australian Competition and Consumer Commission (ACCC) 2002b, *Sweep Report, Sweep #4, Misleading Claims About Health Products*. At, http://www.accc.gov.au/ecom2/netsweep_2002.pdf.

Australian Computer Crime and Security Survey 2003, Australian Federal Police, Queensland Police, South Australia Police, Western Australia Police and AusCERT, Brisbane.

Australian Federal Police 1992, *Annual Report 1991–92*, Australian Federal Police, Canberra.

Australian Federal Police 1993, *Annual Report 1992–93*, Australian Federal Police, Canberra.

Australian Federal Police 1994, *Annual Report 1993–94*, Australian Federal Police, Canberra.

Australian Federal Police 1995, *Annual Report 1994–95*, Australian Federal Police, Canberra.

Australian Federal Police 1996, *Annual Report 1995–96*, Australian Federal Police, Canberra.

Australian Federal Police 1997, *Annual Report 1996–97*, Australian Federal Police, Canberra.

Australian Federal Police 1998, *Annual Report 1997–98*, Australian Federal Police, Canberra.

Australian Federal Police 1999, *Annual Report 1998–99*, Australian Federal Police, Canberra.

Australian Federal Police 2000, *Annual Report 1999–2000*, Australian Federal Police, Canberra.

Australian Federal Police 2001, *Annual Report 2000–01*, Australian Federal Police, Canberra.

Australian Federal Police 2002, *Annual Report 2001–02*, Australian Federal Police, Canberra.

Australian Federal Police 2003, *Annual Report 2002–03*, Australian Federal Police, Canberra.

Australian Institute of Criminology 1999, *Small Business Crime Survey* (computer file), Data held on computer file, Australian Institute of Criminology, Canberra.

Australian Institute of Criminology (AIC) 2003, 'Preventing identity-related fraud', *AICrime Reduction Matters*, No. 14, AIC, 18 November.

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

Australian National Audit Office 1994, *The Australian Government Credit Card: Some Aspects of its Use*, Audit Report No. 1, 1993–94, Project Audit, Australian Government Publishing Office, Canberra.

Australian National Audit Office 2000a, *Magnetic Resonance Imaging Services – Effectiveness and Probity of the Policy Development Processes and Implementation*, Audit Report No. 42 1999–2000, Performance Audit, Australian National Audit Office, Canberra.

Australian National Audit Office 2000b, *Survey of Fraud Control Arrangements in APS Agencies*, Audit Report No. 47 1999–2000, Performance Audit, Australian National Audit Office, Canberra.

Australian Payments Clearing Association 2002, *Payment System Statistics*. At, http://www.apca.com.au/Paymentstatistics.html.

Australian Payments Clearing Association 2003, *Payment System Statistics*. At, http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Payment_Statistics?OpenDocument.

Australian Securities Commission (ASC) 1996, *Phoenix Companies and Insolvent Trading*, ASC Research Report, Sydney.

Australian Securities and Investments Commission 1994, *Annual Report 1993-94*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 1995, *Annual Report 1994-95*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 1996, *Annual Report 1995-96*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 1997, *Annual Report 1996-97*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 1998, *Annual Report 1997-98*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 1999, *Annual Report 1998-99*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2000a, *Annual Report 1999-2000*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2000b, *Report on compliance with the Code of Banking Practice, Building Society Code of Practice, Credit Union Code of Practice and EFT Code of Practice, April 1998 to March 1999*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2001, *Annual Report 2000-01*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2002a, *Annual Report 2001-02*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2002b, *Compliance with the Payments System Codes of Practice and the EFT Code of Conduct, April 2000 to March 2001*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2003a, *Annual Report 2002-03*, Australian Securities and Investments Commission, Sydney.

Australian Securities and Investments Commission 2003b, *Compliance with the Payments System Codes of Practice and the EFT Code of Conduct, April 2001 to March 2002*, Australian Securities and Investments Commission, Sydney.

Australian Transaction Reports and Analysis Centre (AUSTRAC) 1999, 'Great tax results', *AUSTRAC Newsletter*, Spring, p.1.

Australian Transaction Reports and Analysis Centre (AUSTRAC) 2002, *Annual Report 2001–2002*, AUSTRAC, Sydney.

Ayres, I. & Braithwaite, J. 1992, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, New York.

Bachner, B. & Jiang, M. 2000, 'Governing trademarks in cyberspace: A comparative study of the regulation of domain names in China', *Asia Pacific Law Review*, vol. 8, no. 2, pp.191–209.

Bader, J.L. 2001, 'Paranoid lately? You may have good reason', *New York Times Online*, 24 March.

Baker, J. 1996, *Conveyancing Fees in a Comparative Market*, Justice Research Centre and Law Foundation of New South Wales, Sydney.

Bamfield, J. 1998, 'A breach of trust: Employee collusion and theft from major retailers', in *Crime at Work: Increasing the Risk for Offenders*, ed. M. Gill, Perpetuity Press, Leicester, pp.123–42.

Barker, G. 2003a, 'Counterfeit credit card gangs on rise', *Sunday Age*, 17 August, p.7.

Barker, G. 2003b, 'Email frauds hit Westpac customers', *Age*, 15 August, p.7.

BBC Online 1999, 'How Leeson broke the bank', 22 June. At, http://news.bbc.co.uk/1/hi/business/the_economy/375259.stm.

BBC Online 2002, 'What surfers are doing on the net', 11 October. At, http://news.bbc.co.uk/2/hi/technology/2310131.stm.

Bell, C. 2000, *E-Corruption: Exploiting Emerging Technology Corruptly in the New South Wales Public Sector*, unpublished Strategic Assessment, New South Wales Independent Commission Against Corruption, Sydney.

Bell, R.E. 2002, 'The prosecution of computer crime', *Journal of Financial Crime*, vol. 9, no. 4, pp.308–25.

Benitez, M. A. 2002, 'ID card contract awarded', *South China Morning Post* (Hong Kong), 27 February, p.2.

Benson, M.L. 1985, 'Denying the guilty mind: Accounting for involvement in white collar crime', *Criminology*, vol. 23, pp.583–607.

Berinato, S. 2000, 'Are killer hack attacks coming?', ZDNet, 17 December. At, http://www.zdnet.com/zdnn/stories/news/0,4586,2665640,00.html.

Bhojani, S. 2000, 'The professions and whistleblower protections', paper presented at the Australian Institute of Criminology Conference *Crime in the Professions*, Melbourne, 21–22 February.

Biometix 2003, *Summary Report on Biometric Technology*, Australia.

Biometrics Institute 2002, 'An interview with Richard Norton'. At http://www.biometricsinstitute.org/bi/nortoninterview1.htm.

Birmingham, J. 1995, 'Nowhere to hide', *Independent Monthly*, June, pp.45–7.

Blum, R. H. 1972, *Deceivers and Deceived: Observations on Confidence Men and their Victims, Informants and their Quarry, Political and Industrial Spies and Ordinary Citizens*, Charles C. Thomas, Springfield IL

BPay 2003, *BPay News and Views*, Newsletter 003, July 2003. At, http:// www.bpay.com.au/pdfs/BPAY_News_and_Views_Issue_3.pdf.

Braithwaite, J. 1985, 'White collar crime', *Annual Review of Sociology*, vol. 11, pp.1–25.

Braithwaite, J. 1992, 'Penalties for white-collar crime', in *Complex Commercial Fraud*, ed. P.N. Grabosky, Australian Institute of Criminology Conference Proceedings, no. 10, Australian Institute of Criminology, Canberra, pp.167–71.

Braithwaite, J. & Drahos, P. 2000, *Global Business Regulation*, Cambridge University Press, Cambridge.

Bridgeman, J.S. 1997, 'Keynote speech to the electronic shopping forum', *Fair Trading Magazine*, 6 May, Office of Fair Trading, London.

Brown, B. 1998, *Scams and Swindlers: Investment Disasters and How to Avoid Them*, Centre for Professional Development, Australian Securities and Investments Commission, Sydney.

Brown, R. & Johnston, M. 2000, 'Internet fraud sweep fails to turn up any NZ sites', *IDG-Net*, 27 March. At, http://idg.net.nz/webhome.nsf/UNID/ 35166639324 F7B5DCC2568AC0010C1D3!opendocument.

Butler, A. 1996, 'Regulation of content of online information services: Can technology itself solve the problem it has created?' *University of New South Wales Law Journal*, vol. 19, no. 2, pp.193–221.

Campbell, R. 1999, 'DOFA review in wake of alleged $8m fraud', *Canberra Times*, 17 February, pp.1–2.

Campbell, R. 2003, 'Two fraud accuseds acquitted', *Canberra Times*, 11 September, p.8.

Cant, S. 2001, 'New digital ID on the way', *The Age*, 20 March, IT1 p.6.

Carcach, C. & Makkai, T. 2002, *Review of Victoria Police Crime Statistics: A Report Prepared by the Australian Institute of Criminology for the Chief Commissioner, Victoria Police*, Australian Institute of Criminology, Canberra.

Casey, M. 2002, 'Technology that's ready to get under your skin', *Daily Telegraph*, 13 February, p.33.

Cassella, S. D. 2002, 'The recovery of criminal proceeds generated in one nation and found in another', *Journal of Financial Crime*, vol. 9, no. 3, pp.268–276.

Cauchi, S. 1999, 'Psychiatrist accused of $1m fraud', *Age*, 6 January, p.5a.

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

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

Challinger, D. 1996, 'Refund fraud in retail stores', *Security Journal*, vol. 7, pp.27–35.

Chapman, A. & Smith, R.G. 2001, 'Controlling financial services fraud', *Trends and Issues in Crime and Criminal Justice*, No. 189, Australian Institute of Criminology, Canberra.

Charlton, K. & Taylor, N. 2003, 'Online credit card fraud against small businesses', *Research and Public Policy Series*, Australian Institute of Criminology, Canberra.

Churchill, D. 1997, 'Tricks of the trade', *Police Review*, vol. 105, no. 5435, pp.24–5.

CJS Online 2003, 'New offence to tackle organised crime and terrorism', *CJS Online.* At, http://www.cjsonline.gov.uk.

Clarke, R. 1994, 'Human identification in information systems: Management challenges and public policy issues', *Information Technology and People*, vol. 7, no. 4, pp.6–37. At, http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html.

Clarke, R. 2000, 'Submission to the Inquiry into the *Privacy Amendment (Private Sector) Bill* 2000 by the Senate Legal and Constitutional Legislation Committee', 7 September. At, http://www.anu.edu.au/people/Roger.Clarke/ DV/SenatePBSub2000.html.

Clough, J. & Mulhern, C. 2002, *The Prosecution of Corporations*, Oxford University Press, Melbourne.

Comfraud Bulletin 1998, 'Prosecution of largest nursing home fraud in Australian history', *Comfraud Bulletin*, vol. 9, April, p.3.

Commonwealth Attorney-General's Department 2002, *Commonwealth Fraud Control Guidelines*, 13 May 2002. At, http://www.law.gov.au/aghome/ commprot/ crjd/LECD/guidelinesmay.ht.

Commonwealth Consumer Affairs Advisory Council 2002, *Consumer Issues and Youth: A Research Report Into Best Practice in Consumer Education Targeting Young Australians*, July. At, http://www.consumersonline.gov.au/pdfs/youth_jul2002.pdf.

Commonwealth Director of Public Prosecutions 2002, *Annual Report 2001-2002*, Commonwealth Director of Public Prosecutions, Canberra.

Computer Security Institute 2002, '2002 CSI/FBI computer crime and security survey', *Computer Security Issues and Trends*, vol. 8, no. 1, Spring.

Consumer Affairs Victoria 1999, 'Internet service provider disappears into thin cyberspace', *Media release*, 6 May. At, http://www.consumer.vic.gov.au/ cbav/fairsite.nsf/ 5a5c2294e2ee3a664a25678a0013c2bd/ec41ff83a5b98cb5ca25687e0013705b?OpenDocument.

Consumer Affairs Victoria 2001a, 'Thomson urges young people to become savvier consumers', *Media release*, 27 April. At, http://www. consumer.vic.gov.au/ cbav/ fairsite.nsf/5a5c2294e2ee3a664a25678a0013c2bd/2a589556e3b4c841ca256a55001e4244?OpenDocument.

Consumer Affairs Victoria 2001b, 'Minister warns on bogus relief funds for American crisis', *Media release*, 18 September. At, http://www.consumer. vic.gov.au/ cbav/fairsite.nsf/5a5c2294e2ee3a664a25678a0013c2bd/e436496fe4e5b8acca256acc00083971?OpenDocument.

Consumer Affairs Victoria 2002, *M-Commerce. What is it? What Will it Mean for Consumers?* Department of Justice, Melbourne.

Consumer Affairs Victoria, Standing Committee of Officials of Consumer Affairs E-Commerce Working Party 2003, *Web Seals of Approval*, Options Paper, Consumer Affairs Victoria. At, http://www.consumer.vic.gov.au/ cbav/fairattach.nsf/ Images/WebSealsOptionsPaper/$file/WebSealsOptionsPaper.doc.

Consumers International 2000, *Disputes in cyberspace: Online Dispute Resolution for Consumers in Cross-border Disputes – An International Survey*, December. At, http://www.consumersinternational.org/publications/searchdocument.asp? PubID=29.

Cook, V. 1999, 'Trust me, I'm a computer', *Communications Newsletter*, September, pp.14–15.

Council of Europe 2003, *Convention on Cybercrime*. At, http://conventions.coe.int/Treaty/ENCadreListeTraites.htm.

Cowan, S. & Eliot, L. 2003, '$19m thief may get more jail', *West Australian*, 4 November.

Cox, R. J. & Wallace, D.A. (eds) 2002, *Archives and the Public Good: Accountability and Records in Modern Society*, Quorum Books, Westport Connecticut.

Cressey, D.R. 1953, *Other Peoples Money: A Study in the Social Psychology of Embezzlement*, Free Press, Glencoe IL.

Cressey, D.R. 1986, 'Why managers commit fraud', *Australian and New Zealand Journal of Criminology*, vol. 19, pp.195–209.

Criminal Justice Commission, Queensland 1993, *Corruption Prevention Manual*, Criminal Justice Commission, Brisbane.

Crofts, P. 2002, *Gambling and Criminal Behaviour: An Analysis of Local and District Court Files*, A Research Project for the Casino Community Benefit Fund, Sydney.

Crompton, M. 2002, 'Biometrics and privacy: The end of the world as we know it or the white knight of privacy?' paper presented at Biometrics-Security and Authentication Biometrics Institute Conference in Sydney, 20 March 2002.

Cuganesan, S. & Lacey, D. 2003, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, SIRCA, Sydney.

Dancer, H. 2000, 'K2 uncovers GST keyhole', *The Bulletin*, 11 July, p.76.

Day, C. 2000, 'Fraud control in the Australian Defence organisation', paper presented at the Australian Institute of Criminology Conference *Crime in the Professions*, Melbourne, 21–22 February.

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.

Dearne, K. 2002, 'ISPs lead fraud crackdown', *Australian*, 12 February, p.25.

De Maria, W. 1995, 'Whistleblowing', *Alternative Law Journal*, vol. 20, no. 6, pp.270–81.

Denning, D. E. 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.

Department of Communications, Information Technology and the Arts (DCITA) 1999, *Shopping on the Internet: Facts for Consumers*. At, http://www. dcita.gov.au/Article/0,,0_1-2_1-4_13878,00.html.

Department of Infrastructure, Victoria 2002, *About DOI: Whistleblowers Protection Act 2001*. At, http://www.doi.vic.gov.au/doi/internet/home.nsf/ headingpagesdisplay/ about+uswhistleblowers+protection+act.

Department of Justice, United States 1999, *Report of the Computer Crime and Intellectual Property Section, Working Group on Unlawful Conduct on the Internet*. At, http:// www.cybercrime.gov/index.html.

Department of Justice, United States 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section. At, http://www.cybercrime.gov/append.htm.

Department of Justice, Victoria 2002, *Procedures Under the Whistleblowers Protection Act 2001*, Department of Justice. At, http://www.justice.vic.gov.au/legalchannel/ dojsite.nsf/dab0606eefd3be6bca256ab0003f4687/16c44eb612cd81 deca256c1300790fd3/$FILE/DOJWhistleblowersProcedures_Jul02.pdf.

Department of Public Works and Services, New South Wales 1999, *Electronic Procurement: Taking Up the Challenge*, Sydney.

Department of Treasury, Consumer Affairs Division, Australia 2000, *Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business*, Commonwealth of Australia, Canberra.

Department of Treasury and Finance, Victoria 2002, 'EC4P: The Victorian Government's electronic procurement project', State Government of Victoria. http://www.ec4p.dtf.vic.gov.au/domino/web_notes/ec4p/ec4p.nsf/ 0/f3acbc 234ff76 a45ca256c3a0016a4bc/$FILE/EC4P_brochFINAL.pdf.

Department of Treasury and Finance, Victoria 2003a, *Whole of Government Financial Management Compliance Framework: Explanatory Framework Document*, State Government of Victoria.

Department of Treasury and Finance, Victoria 2003b, *Standing Directions*, State Government of Victoria

Dix, A. 2002, 'Crime and misconduct in the medical profession', in *Crime in the Professions*, ed. R.G. Smith, Ashgate, Aldershot, pp.67–98.

Duffield, G. & Grabosky, P. 2001, 'The psychology of fraud', *Trends and Issues in Crime and Criminal Justice*, no. 199, Australian Institute of Criminology, Canberra.

Dunstone, T. 2003, 'The use of biometric technology in airports', At, http://www. biometricsinstitute.org/bi/Articles/0303_AirportReview1.pdf.

Dyson, D.I.C. 2003, 'Crimes of deception – Recent cases of identity theft and fraud', paper presented at the Financial Crimes Summit, Sydney Marriot Harbourside, Sydney.

Elliott, G. 2003, 'Enron executive in chains', *Australian*, 12 September, p.17.

Elliott, I. 1980, 'Dishonesty in Victoria – The Queen v Salvo', *Criminal Law Journal*, vol. 4, pp.149–68.

Ernst & Young 1998, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

Ernst & Young 2000, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

Ernst & Young 2003, *Fraud: The Unmanaged Risk*, Ernst & Young, Johannesburg.

European Commission 2002, 'Data protection: Commission decisions on the adequacy of the protection of personal data in third countries', European Commission. At, http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm.

European Commission 2003, 'Commission decisions on the adequacy of the protection of personal data in third countries', European Commission. At, http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.

Farrant, D. 1999, 'Pre-paid funeral payments misused', *The Age*, 24 July, p.10.

Federal Bureau of Investigation, United States 2000, *Press Release*, 14 August http://www.fbi.gov/pressrm/pressrel/pressrel100/vatis08142000.htm.

Federal Trade Commission, United States 2002, 'Sentinel top complaint categories: January 1–December 31, 2001', Federal Trade Commission, January 7. At, http://www.consumer.gov/sentinel/images/charts/top2001.pdf.

Federal Trade Commission, United States 2003, 'Sentinel complaints by calendar year', Federal Trade Commission, 22 January, http://www.consumer.gov/sentinel/sentinel-trends/page3.pdf.

Fisse, B. 1990, *Howard's Criminal Law*, 5th edn, Law Book Company, Sydney.

Fisse, B. & Braithwaite, J. 1993, *Corporations, Crime and Accountability*, Cambridge University Press, Cambridge.

Fitzsimmons, C. 2002, 'Visa pays for swipe at fraud', *Australian*, October 14, p.9.

Fletcher, J. 1998, 'National influences on the regulation of professional conduct', in *Health Care, Crime and Regulatory Control*, ed. R.G. Smith, Hawkins Press, Sydney, pp.72–9.

Forde, P. & 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. At, http://www.cbs.curtin.edu.au/Workingpapers/other/ Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20 Criminals.doc.

Fox, R. & Freiberg, A. 1999, *Sentencing: State and Federal Law in Victoria*, 2nd edn, Oxford University Press, Melbourne.

Freauf, M. A. 1996, 'Refund fraud', *Australian Police Journal*, vol. 50, no. 2, pp.64–7.

Freiberg, A. 1992, 'Sentencing white-collar criminals', in *Sentencing of Federal Offenders,* Proceedings of the Australian Institute of Judicial Administration (AIJA) Seminar for judges and magistrates held 1–2 November 1991, AIJA, Melbourne, pp.1–19.

Freiberg, A. & Ross, S. 1999, *Sentencing Reform and Penal Change: The Victorian Experience*, Federation Press, Sydney.

Geis, G. 1991, 'White-collar crime: What is it?' *Current Issues in Criminal Justice*, vol. 3, no. 1, pp.–24.

Gettler, L. 2000, 'New rules to put heat on fraud', *Age*, 15 April 2000, p.(4)2.

Gips, M. 1998, 'Where has all the money gone?' *Security Management*, vol. 42, no. 2, pp.32–40.

Glasner, J. 2002, 'Wanna bet? Feds say not so fast', *Wired News*, 3 October. At, http://www.wired.com/news/business/0,1367,55510,00.html.

Grabosky, P.N. 1984, 'Corporate crime in Australia: An agenda for research', *Australian and New Zealand Journal of Criminology*, vol. 17, pp.95–107.

Grabosky, P.N. 1995, 'Regulation by reward: On the use of incentives as regulatory instruments', *Law and Policy*, vol. 17, no. 3, pp.257–82.

Grabosky, P.N. & Smith, R.G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney / Transaction Publishers, New Brunswick.

Grabosky, P.N., Smith, R.G. & Dempsey, G. 2001, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Gray, D. 2000, 'HIC chases $164,000 over suspect scans', *Age*, 13 April, p.6.

Gray, G. 1999, 'The changing face of legal practice and implications for professional indemnity insurance', *Insurance Law Journal*, vol. 11, no. 1, pp.72–90.

Hall, T. 1979, *White-collar Crime in Australia*, Harper and Row, Sydney.

Hardt, M. & Negri, A. 2000, *Empire*, Harvard University Press, Cambridge MA.

Health Insurance Commission (HIC) 1997, *Annual Report 1996–97*, Health Insurance Commission, Canberra.

Health Insurance Commission (HIC) 1998, *Annual Report 1997–98*, Health Insurance Commission, Canberra.

Health Insurance Commission (HIC) 2001a, *Annual Report 2000–01*, Health Insurance Commission, Canberra. Also at, http://www.hic.gov.au/ annualreport/.

Health Insurance Commission (HIC) 2001b, 'Second Victorian pharmacist sentenced over involvement in major $1.3m PBS fraud', *Media release*, 6 July. At, http://www.hic.gov.au/CA256995000C9DAE/page/Media+Room-Media+Releases-06+Jul+2001+%282%29?OpenDocument&1=65-Media+Room~&2=15-Media+Releases~&3=75-06+Jul+2001+(2)~.

Hirschman, A.O. 1970, *Exit, Voice and Loyalty: Responses to Decline in Firms, Organisations and States*, Harvard University Press, Cambridge MA.

Holding Redlich 2002, 'Reference checks: Meeting your obligations', *Employment and Industrial Relations: Update*, Autumn. At, http://www.holdingredlich.com.au/newsletter/HOL_305_EIR_law_aut.02.pdf.

Home Office, Britain 2002, *Entitlement Cards Unit Website*. At, http://www.homeoffice.gov.uk/dob/ecu.htm.

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

Hughes, G. 1989, 'Legislative responses to computer crime', *Law Institute Journal*, June, pp.507–9.

Hume, J. 1996, 'Stamping out staff theft', *Security Australia*, vol. 16, no. 11, pp.24–8.

IFAC International Auditing and Assurance Board 2003, 'The auditor's responsibility to consider fraud in an audit of financial statements', *Proposed Revised International Standard on Auditing 240*, August. At, http://www.ifac.org/Guidance/EXD-Details.php?EDID=0023.

Inspector General of Penal Establishments 1855, *Annual Report for the Year Ending 30 September 1855*, Government Printer, Melbourne.

Insurance Council of Australia 1994, *Insurance Fraud in Australia*, Insurance Council of Australia, Sydney.

International Biometrics Group 2003, *Biometric Market Report 2003-2007*, International Biometrics Group, New York.

International Marketing Supervision Network 2002, *IMSN Activities*. At, http://www.imsnricc.org/imsn/activities.htm.

Internet Fraud Complaint Center 2001a, *Internet Fraud Preventive Measures*. At, http://www1.ifccfbi.gov/strategy/fraudtips.asp.

Internet Fraud Complaint Center 2001b, *Internet Auction Fraud*, May. At, http://www1.ifccfbi.gov/strategy/AuctionFraudReport.pdf.

Internet Fraud Complaint Center 2002, *IFCC 2001 Internet Fraud Report*. At, http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf.

Internet Fraud Complaint Center 2003, *IFCC 2002 Internet Fraud Report*. At, http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

Internet Fraud Watch 2002, *2001 Internet Fraud Statistics*. At, http://www.fraud.org/internet/2001stats.htm.

Internet Fraud Watch 2003, *2002 Internet Fraud Statistics*. At, http://www.fraud.org/2002intstats.htm.

Internet Industry Association 2001, *Interactive Gambling Industry Code*, December. At, http://www.iia.net.au/gamblingcode.html.

James, M. 2000, 'Art crime', *Trends and Issues in Crime and Criminal Justice*, No. 170, Australian Institute of Criminology, Canberra.

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

Johnson, T. J. 1972, *Professions and Power*, Macmillan Press, London.

Joyce, A. 1999, 'Cautionary tales of Commonwealth credit card fraud', *Comfraud Bulletin*, vol. 12, January, pp.2, 4.

Kapardis, M. & Monroe, G.S. 1999, 'Major fraud by people in positions of financial trust in Australia', *Balkan Law Review*, vol. 3, no. 1.

Keenan, A. 2002, 'Internet stalkers face 10 years jail', *The Australian*, 14 October, p.9.

Kennedy, l. 2002, 'A scam to bring the house down', *Sydney Morning Herald*, 28 August. Also at, http://www.smh.com.au/articles/2002/08/27/1030053059530.html.

Khoury, D. 1990, 'The statute of frauds revisited', *Law Institute Journal*, September, pp.822–3.

Kinnear, P. & Graycar, A. 1999, 'Abuse of older people: Crime or family dynamics?', *Trends and Issues in Crime and Criminal Justice*, No. 113, Australian Institute of Criminology, Canberra.

KPMG 1997, *Fraud Survey 1997*, KPMG, Sydney.

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

KPMG 2001, *Global efr@ud Survey*, KPMG Forensic and Litigation Services.

KPMG 2002, *Fraud Survey 2002*, KPMG, Sydney.

Krambia-Kapardis, M. 2001, *Enhancing the Auditor's Fraud Detection Ability: An Interdisciplinary Approach*, Peter Lang, Frankfurt am Main.

Kriegler, R. 1999, 'LIV annual survey of legal practitioners', *Law Institute Journal*, March, pp.52–7.

Kurrle, S., Sadler, P. & Cameron, I. 1992, 'Patterns of elder abuse', *Medical Journal of Australia*, vol. 157, no. 10, pp.673–6.

Kwakernaak, K. 2003, 'Internet security: Emerging technologies and customer acquiring', paper presented at the Financial Crimes Summit 2003, Sydney, 29–30 May.

Lanham, D., Weinberg, M., Brown, K.E. & Ryan, G.W. 1987, *Criminal Fraud*, Law Book Company, Sydney.

Lapthorne, K. 2003, 'Data whiz gets jail', *Herald Sun*, 20 September.

Law Commission, Britain 1999, *Legislating the Criminal Code: Fraud and Deception: A Consultation Paper*, Law Commission, London.

Law Commission, New Zealand 1998, *Electronic Commerce Part 1: A Guide for the Legal and Business Community*, Report No. 50, October. At, http://www.lawcom.govt.nz/content/publications/r50.pdf.

Leamy, R. 1997, 'False invoices: Don't get stung', *Compliance*, August, pp.2–5. At, http://www.comcom.govt.nz/publications/GetFile.CFM?Doc_ID=58&Filename=CAUG97.PDF.

Legal Practice Board 2001, *Annual Report 2000–2001*, Legal Practice Board, Melbourne.

Legal Practice Board 2002, *Annual Report 2001–2002*, Legal Practice Board, Melbourne.

Lehman, D. 2000, 'Feds ID hacker who stole 485,000 credit-card numbers', *InfoWorld Daily News*, InfoWorld Media Group Inc. At, http://www,infoworld.com (available from http://www.factiva.com (subscriber only)).

Levi, M. 1981, *The Phantom Capitalists*, Heinemann, London.

Lipton, J. 1998, 'Property offences in the electronic age', *Law Institute Journal*, October, pp.54–58.

Louis Harris & Associates Inc. 1999, *Consumers and the 21st Century: A Survey Conducted for the National Consumers League*, Louis Harris & Associates Inc, New York.

Lozusic, R. 2003, *Identity Fraud: Briefing Paper*, New South Wales Parliamentary Library, Sydney.

McAuliffe, W. 2002, 'Asylum seekers get first UK biometric ID cards', *ZDNet Australia*, 5 February. At, http://www.zdnet.com.au/newstech/security/story/0,2000024985,20263301,00.htm.

McConvill, J. 2001, 'Contemporary comment: Computer trespass in Victoria', *Criminal Law Journal*, vol. 25, pp.220–227.

Mackenzie, S. 2002, 'Organised crime and common transit networks', *Trends and Issues in Crime and Criminal Justice*, No. 233, Australian Institute of Criminology, Canberra.

McKindley, I 2003, 'An update on card-not-present crime', paper presented at the Financial Crimes Summit 2003, Sydney, 29–30 May.

Mackrell, N. 1996, 'Economic consequences of money laundering', in *Money Laundering in the 21st Century: Risks and Countermeasures*, eds A. Graycar & P. Grabosky, Australian Institute of Criminology, Canberra, pp.29–35.

Mansfield, A.J. & Wayman, J.L. 2002, *Best Practices in Testing and Reporting of Biometric Devices: Version 2.01*, Centre for Mathematics and Scientific Computing, National Physical Laboratory, Middlesex.

Mansfield, T., Kelly, G., Chandler, D. & Kane, J. 2001, *Biometric Product Testing Final Report*, Issue1.0, 19 March, Centre for Mathematics and Scientific Computing, National Physical Laboratory, Middlesex.

Markoff, J. 2001, 'Warning from Microsoft on false digital signatures', *New York Times Online*, 23 March.

Mayhew, P. 2003, *Counting the Costs of Crime in Australia: Technical Report*, Technical and Background Paper Series No 4, Australian Institute of Criminology, Canberra. At, http://www.aic.gov.au/publications/tbp/tbp004.html.

Medical Practitioners Board of Victoria 1995, *Annual Report 1995*, Medical Practitioners Board of Victoria, Melbourne.

Medical Practitioners Board of Victoria 1996, *Annual Report 1996*, Medical Practitioners Board of Victoria, Melbourne.

Medical Practitioners Board of Victoria 2002, *Annual Report 2001–02*, Medical Practitioners Board of Victoria, Melbourne.

Meijboom, A.P. 1988, 'Problems related to the use of EFT and teleshopping systems by the consumer', in *Telebanking, Teleshopping and the Law*, eds Y. Poullet & G.P.V. Vandenberghe, Kluwer, Deventer, pp.23–32.

Mills, J. 1999, 'Ethics in governance: Developing moral public service', *Journal of Financial Crime*, vol. 7, no. 1, pp.52–62.

Minister for Finance, Victoria 2001, 'New era of openness for whole of Government: Kosky', *Media release*, 7 May. At, http://www.ec4p.dtf.vic.gov.au/domino/web_notes/ec4p/ec4p.nsf/WebDocs/E3046B61E4098BED4A256AD100261993.

Ministerial Council on Consumer Affairs 2003, *Strategic Agenda 2003–2004*. At, http://www.consumer.gov.au/html/mcca_projects.htm.

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 1995, *Theft, Fraud, Bribery and Related Offences: Report, Chapter 3*, Commonwealth Attorney-General's Department, Canberra.

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2001, *Damage and Computer Offences: Report, Chapter 4*, Commonwealth Attorney-General's Department, Canberra.

Multimedia Victoria 1998, *Promoting Electronic Business: Electronic Commerce Framework Bill*, A Discussion Paper, July, Melbourne. At, http://www.egov.vic.gov.au/pdfs/Comm.pdf.

National Office for the Information Economy (NOIE) 2000, *E-Commerce: Beyond 2000*, NOIE, Canberra. At, http://www.noie.gov.au/publications/NOIE/ecommerce_analysis/beyond2k_final_report.pdf.

National Office for the Information Economy (NOIE) 2002, *Online Authentification*, NOIE, Canberra.

National Office for the Information Economy (NOIE) 2003a, *Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered*, Canberra, National Office for the Information Economy, Canberra.

National Office for the Information Economy (NOIE) 2003b, *Gatekeeper Frequently Asked Questions*, NOIE, Canberra, http://www.noie.gov.au/projects/confidence/Securing/FAQs.htm.

Needham, K. 2000, 'It's a tangled web they thieve', *Sydney Morning Herald*, 25 October 2000.

Nettler, G. 1974, 'Embezzlement without problems', *British Journal of Criminology*, vol. 14, pp.70–7.

Nettler, G. 1982, *Lying, Cheating, Stealing*, Anderson Publishing, Cincinnati.

Nettleton, J. 2002, 'Internet gambling regulation in Australia', *World Online Gambling Law Report*, vol. 1, no. 6, September. See http://www.e-comlaw.com/woglr/ (subscription only).

Neumann, A.L. 2001, 'The great firewall', *CPJ Briefings*, January. At, http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html.

Neville, L. 2000, 'Crime and misconduct amongst solicitors in Victoria', paper presented at the Australian Institute of Criminology Conference 'Crime in the Professions', Melbourne, 21–22 February.

New, M. 2003, 'How can the use of chip technology help in controlling fraud?', paper presented at the Financial Crimes Summit 2003, Sydney, 29–30 May.

Newlan, D. 2000, 'Detecting and preventing fraud in the energy and natural resources sector', *Energy and Natural Resources Newsletter*, KPMG, Sydney.

New South Wales Audit Office 1994, *Fraud Control: Developing an Effective Strategy*, Audit Office of NSW, Sydney.

New South Wales Audit Office 1999, *Self-Audit Guide: Fraud Con*trol, 3rd edn, Audit Office of NSW, Sydney.

New South Wales Independent Commission Against Corruption (ICAC) 1992, *Report on Unauthorised Release of Government Information*, ICAC, Sydney.

New South Wales Independent Commission Against Corruption (ICAC) 1999, *Investigation into Sydney Ferries: Dishonest Creation and use of 'Live' Tickets by Former Staff of Sydney Ferries at Manly Wharf from 1994 to 1997*, NSW ICAC, Sydney.

New South Wales Law Reform Commission 2001, *Surveillance – An Interim Report*, Report 98, published by the NSW Law Reform Commission in Sydney. At, http://www.lawlink.nsw.gov.au/lrc.nsf/pages/r98toc.

New South Wales Legislative Council 2002, *Debates* (*Hansard*), Article No.25 of 12 June (Corrected copy).

New South Wales Medical Board 1993, *Annual Report for the Period Ended 31 March 1993*, New South Wales Medical Board, Gladesville NSW.

New Yorker 1993, July edition, p.61.

Noble, H.B. 1999, 'Hailed as a surgeon general, Koop criticised on Web ethics', *New York Times*, September 4.

Office of the Federal Privacy Commissioner 2000, *Guidelines on Workplace E-mail, Web Browsing and Privacy*, 30 March. At, http://www.privacy.gov.au/ internet/E-mail/index.html.

Office of Government Information Technology 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, Office of Government Information Technology, Canberra.

Office of Public Employment, Victoria 2002a, *Code of Conduct for the Victorian Public Sector*, Melbourne. At, http://www.ope.vic.gov.au/ope/ope.nsf/ web+pages/ E5969E88E8421559CA256C14000AC695/$file/Code2002.doc.

Office of Public Employment, Victoria 2002b, *Guidelines for Disclosures Under the Whistleblowers Protection Act 2001*, Melbourne. At, http://www.ope.vic.gov.au/ OPE/OPE.nsf/e08c0750d2add85e4a25642100132fce/26bda3df47c5ae1c4a256b2c 001a03b5?OpenDocument.

Office of Public Employment, Victoria 2003, *Code of Conduct for the Victorian Public Sector*, Melbourne. At, http://www.ope.vic.gov.au/ope/ope.nsf/web+pages/ E5969E88E8421559CA256C14000AC695/$file/Code2003.doc.

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

Organisation for Economic Co-operation and Development 1999, *Recommendation of the Council of the OECD Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December, OECD, Paris. At, http://www.oecd. org/oecd/pages/home/displaygeneral/0,3380,EN-document- 0-nodirectorate-no-24-320-0,FF.html.

Page, F. 1997, 'Defining fraud: An argument in favour of a general offence of fraud', *Journal of Financial Crime*, vol. 4, no. 4, pp.287–308.

Parker, C. 1997, 'Justifying the New South Wales legal profession 1976 to 1997', *Newcastle Law Review*, vol. 2, no. 2, pp.1–29.

Parliament of Victoria, Law Reform Committee 1995, *Curbing the Phoenix Company: Second Report on the Law Relating to Directors and Managers of Insolvent Corporations*, Government Printer, Melbourne.

Parliament of Victoria, Law Reform Committee 1999, *Technology and the Law*, (52nd Session, 1998–99), Government Printer, Melbourne.

Parliamentary Debates, Victoria 2000a, *Electronic Transactions (Victoria) Bill*, Legislative Assembly, Second Reading Speech, the Hon. John Brumby, 6 April, p.778. At, http://tex2.parliament.vic.gov.au/bin/texhtmlt?form=VicHansard. dumpall&db=hansard91&dodraft=0&speech=5087&activity=Second+ Reading&title=ELECTRONIC+TRANSACTIONS+%28VICTORIA%29+BILL& date1=6&date2=April&date3=2000.

Parliamentary Debates, Victoria 2000b, *Electronic Transactions (Victoria) Bill*, Legislative Assembly, Second Reading Debate, the Hon. Victor Perton, 3 May, p.1217. At, http://tex.parliament.vic.gov.au/bin/texhtmlt?form=VicHansard. dumpall&db= hansard91&dodraft=0&speech=5605&activity=Second+ Reading&title=ELECTRONIC+ TRANSACTIONS+%28VICTORIA%29+BILL& date1=3&date2=May&date3=2000.

Parliamentary Debates, Australia 2001, *Interactive Gambling Bill* 2001 (Cth), Senate, Second Reading Speech, Senator Ian Campbell, 5 April, p.23750. Also at, http://www.aph.gov.au/hansard/senate/dailys/ds050401.pdf.

Pearson, G. 1996, 'Naked men, food and water: Marketing law and codes of practice', *Current Commercial Law*, vol. 4, no. 1, pp.21–32.

Pitsis, S. 2003, 'Three years for $19m bank fraud', *The Australian*, 30 October, p.4.

Potter, E.J. 2002, 'Customer authentication: The evolution of signature verification in financial institutions', *Journal of Economic Crime Management*, vol. 1, no. 1, Summer. Also at, http://www.jecm.org/02_vol1_issue1_art2.pdf.

PricewaterhouseCoopers 2002, *Intellectual Property Loss Survey Report 2001*, PricewaterhouseCoopers, Melbourne.

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

Privacy International 2002, *Entitlement Card Proposal FAQ*. At, http://www.privacy international.org/issues/idcard/uk/uk-idcard-faq.html.

Robinson, R. 2002, 'New Laws Likely to Ban Net Stalking', *Herald Sun*, 21 September. At, http://heraldsun.news.com.au/common/story_page/0,5478,5138409%25 5E11869,00.html.

Rosoff, S.M., Pontell, H.N. & Tillman R.1998, *Profit Without Honor: White Collar Crime and the Looting of America*, Prentice Hall Inc., Upper Saddle River, New Jersey.

SAI Global Assurance Services 2003, *Information Security Management: Are you protecting your company's information?* At, http://www.sai-global.com/ASSURANCE/ SECTIONS/InfoSecurityManagement/BrochureInformationSecurity.pdf.

Sakurai, Y. & Smith, R. G. 2003, 'Gambling as a motivation for the commission of financial crime', *Trends and Issues in Crime and Criminal Justice*, No. 256, Australian Institute of Criminology, Canberra.

Sampford, C. & Blencowe, S. 2002, 'Raising the standard: An integrated approach to promoting professional values and avoiding professional criminality', in *Crime in the Professions*, ed. R.G. Smith, Ashgate, Aldershot, pp.251–68.

Sarre, R. 1995, 'Keeping an eye on fraud: Proactive and reactive options for statutory watchdogs', *Adelaide Law Review*, vol. 17, pp.283–300.

Securities and Exchange Commission 2002, 'Regulators launch fake scam web sites to warn investors about fraud'. At, http://www.sec.gov/news/press/2002-18.txt.

Seltzer, W. 1998, 'Population statistics, the Holocaust, and the Nuremberg Trials', *Population and Development Review*, vol. 24, no. 3, pp.511–552.

Sennewald, C.A. & Christman, C.P.P. 1992, *Shoplifting*, Butterworth Heinneman, Boston.

SET Secure Electronic Transaction LLC 2003. At, http://www.setco.org/.

Sexton, J. 2003, 'I'm not Jane, rort victim tells Telstra', *Weekend Australian*, 5 July, p.9.

Shiel, F. 2003, 'New legal complaints system touted', *The Age*, 6 June, p.2.

Slane, B. 2001, 'Catching the fast slithering tail of e-privacy', Address by the Privacy Commissioner of New Zealand to IIR *Web Law Conference*, Auckland, 25–26 June.At, http://www.privacy.org.nz/news5.html.

Smith, R.G. 1991, '"Strangers withdraw!": The use of in camera hearings by the Professional Conduct Committee of the General Medical Council', *Professional Negligence*, vol. 7, no. 4, pp.178–83.

Smith, R.G. 1993, 'The development of ethical guidance for medical practitioners by the General Medical Council', *Medical History*, vol. 37, pp.56–67.

Smith, R.G. 1994, *Medical Discipline*, Clarendon Press, Oxford.

Smith, R.G. 1999, 'Internet payment systems and their security risks', *Journal of Financial Crime*, vol. 7, no. 2, pp.155–60.

Smith, R.G. 2000, 'Fraud and financial abuse of older persons', *Current Issues in Criminal Justice*, vol. 11, no. 1, pp.8–26.

Smith, R.G. 2002a, *Crime in the Professions*, Ashgate, Aldershot.

Smith, R.G. 2002b, 'White-collar crime', in *The Cambridge Handbook of Australian Criminology*, eds A. Graycar & P. Grabosky, Cambridge University Press, Cambridge, pp.126–56.

Smith, R.G. & Grabosky, P.N. 1998, *Taking Fraud Seriously: Issues and Strategies for Reform*, Institute of Chartered Accountants in Australia, Fraud Advisory Council, Sydney.

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

Smith, R.G. & 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.

Smith, R.G., Wolanin, N. & Worthington, G. 2003, 'e-Crime solutions and crime displacement', *Trends & Issues in Crime and Criminal Justice*, No. 243, Australian Institute of Criminology, Canberra.

Sorkin, D.E. 2001, 'Payment methods for consumer-to-consumer online transactions', *Akron Law Review*, vol. 35, pp.1–30. At, http://www.sorkin.org/ articles/akron.pdf.

South Australian Internet Association (SAIA) 2002, *Code of Ethics and Conduct*. At, http://www.saia.asn.au.

South China Morning Post (Hong Kong) 2002, 'ID card plans raise issue of carrier privacy', 17 January, p.11.

Stamp, J. 1929, *Some Economic Factors in Modern Life*, King, London.

Standards Australia 1998, *Compliance Programs*, AS 3806–1998, Standards Association of Australia, Sydney.

Standards Australia 1999, AS/NZS 4360:1999 *Risk Management*, Standards Association of Australia, Sydney.

Standards Australia 2000, HB 231:2000 *Information security risk management guidelines*, Standards Association of Australia, Sydney.

Standards Australia 2001, AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management*, Standards Association of Australia, Sydney.

Standards Australia 2002, 'New national guidelines for corporate governance', *Media release*, 22 August. At, http://www.standards.com.au/catalogue/Script/ GetPage.asp?url=/STANDARDS/NEWSROOM/NEWS%20RELEASE/2002-08-02/2002-08-02.HTM.

Standards Australia 2003a, AS 8000-2003 *Good Governance Principles*, Standards Association of Australia, Sydney.

Standards Australia 2003b, AS 8001-2003 *Fraud and Corruption Control*, Standards Association of Australia, Sydney.

Standards Australia 2003c, AS 8002-2003 *Organizational Codes of Conduct*, Standards Association of Australia, Sydney.

Standards Australia 2003d, AS 8003-2003 *Corporate Social Responsibility*, Standards Association of Australia, Sydney.

Standards Australia 2003e, AS 8004-2003 *Whistleblower Protection Programs for Entities*, Standards Association of Australia, Sydney.

Standards Australia 2003f, AS/NZS 7799.2:2003 *Information security management – Part 2: Specification for information security management systems*, Standards Association of Australia, Sydney.

Standards Australia 2003g, HB 171-2003 *Guidelines for the management of IT evidence*, Standards Association of Australia, Sydney.

Steel, A. 2000, 'The appropriate test for dishonesty', *Criminal Law Journal*, vol. 24, pp.46–59.

Stotland, E. 1977, 'White collar criminals', *Journal of Social Issues*, vol. 33, pp.179–196.

Sullivan, C. 1987, 'Unauthorised automatic teller machine transactions: Consequences for customers of financial institution', *Australian Business Law Review*, vol. 15, no. 3, pp.187–214.

Supreme Court of Victoria 2002, 'Technology in court expands at Supreme Court', *Media Release*, 20 May. At, http://www.supremecourt.vic.gov.au/CA256902000FE154/Lookup/MediaReleases/$file/Media-TechnologyinCourt.pdf.

Sutherland, E. H. 1940, 'White-collar criminality', *American Sociological Review*, vol. 5, pp.1–12.

Sydney Morning Herald 2002a, 'Harris Scarfe man gets six', 27 June. At, http://www.smh.com.au/articles/2002/06/26/1023864606466.html.

Sykes, G.M. & Matza, D. 1957, 'Techniques of neutralization: A theory of delinquency', *American Sociological Review*, vol. 22, pp.664–70.

Tarling, S. 2003, 'E-trial ushers in judgement day for IT', *Sydney Morning Herald*, 23 September. At, http://www.smh.com.au/articles/2003/09/22/1064082912340.html

Taylor, N. 2002, 'Reporting of crime by small retail businesses', in *Trends and Issues in Crime and Criminal Justice*, No. 242, Australian Institute of Criminology, Canberra.

Taylor, N. & Mayhew, P. 2002a, 'Financial and psychological costs of crime for small retail businesses', in *Trends and Issues in Crime and criminal Justice*, No. 229, Australian Institute of Criminology, Canberra.

Taylor, N. & Mayhew, P. 2002b, 'Patterns of victimisation among small retail businesses', in *Trends and Issues in Crime and criminal Justice*, No. 221, Australian Institute of Criminology, Canberra.

Thalheim, L., Krissler, J. and Ziegler, P.M. 2002, 'Body check: Biometrics defeated', *c't magazine*, issue 11, 22 May. At, http://www.heise.de/ct/english/02/11/114/.

Tomasic, R. 1993, *Corporate Law Sanctions and the Control of White-collar Crime*, Centre for National Corporate Law Research, University of Canberra, Canberra.

Tomazin, F. 2001, 'Internet fraud man sentenced', *Age*, 23 May 2001.

Tonking, A.I. 1995, 'Implications for the legal profession in competition policy reforms', *Law Society Journal*, vol. 33, no. 7, pp.38, 40–2.

Transparency International 2002, *Corruption Perception Index 2002*. At, http://www.transparency.org/cpi/index.html.

Tweney, D. 1998, 'Sex scam points out lack of safeguards in online business', 3 August. At, http://www.tweney.com/prophet/980803prophet.htm.

Tyree, A.L. 1990, *Banking Law in Australia*, Butterworths, Sydney.

Underwood, G. 2003, 'Implementing an effective fraud control strategy and learning about the use of fraudulent documents in financial Applications', paper given at Financial Crimes Summit, Sydney Marriott Harbourside, Sydney.

UK Biometrics Working Group 2002, 'Use of biometrics for identification: Advice on product selection'. At, http://www.cesg.gov.uk/site/ast/biometrics/media/Biometrics%20Advice.pdf.

United States General Accounting Office (GAO) 2002, *Technology Assessment: Using biometrics for border security,* GAO-03-174, November, Washington DC. At, http://www.gao.gov/new.items/d03174.pdf. United States President (George W. Bush) 2002, *Securing the Homeland, Strengthening the Nation*, Office of the President, Washington. At, http://www.whitehouse. gov/ homeland/ homeland_security_book.html.

United States, President's Critical Infrastructure Protection Board 2002, *The National Strategy to Secure Cyberspace (Draft)*, President's Critical Infrastructure Protection Board, Washington. http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf.

Urban, R. 2003, Police raids seize DVDs', *Sunday Age*, 7 September, p.3.

Van Kesteren, J., Mayhew, P., Nieuwbeerta, P. & Bruinsma, G. 2000, *Criminal Victimisation in Seventeen Industrialised Countries: Key Findings from the 2000 International Crime Victims Survey*, WODC, Ministry of Justice, The Hague. At, http://www.unicri.it/icvs/publications/pdf_files/key2000i/index.htm.

Victoria Police 1960–2003, *Statistical Review of Crime 1960–2003*, Victoria Police, Melbourne.

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

Victorian Auditor-General's Office 2000 – *Auditing in the Public Interest* (provided as an attachment to Submission 3).

Victorian Government Purchasing Board 2001, *Government Contracting and Purchasing: Purchasing Rules: A Quick Reference* Department of Treasury and Finance. At, http://www.vgpb.vic.gov.au/polguid/worddoc/purchasingrules.pdf.

Victorian Government Purchasing Board 2002, *General Government Purchasing Card: Rules for Use and Administration*, State of Victoria. At, http://www.dtf.vic.gov.au/dtf/RWP323.nsf/0/3b51cd2edfd3ae6f4a2569de0018cfb0/$FILE/GGPC.pdf.

Visa International 2001. At, http://www.visa.com.

Visa International 2003. At, http://international.visa.com/fb/paytech/secure/main.jsp.

Walker, J. 1994, *The First Australian National Survey of Crimes Against Businesses*, Australian Institute of Criminology, Canberra.

Walker, J. 1995, *Estimates of the Extent of Money Laundering in and through Australia*, Prepared for the Australian Transaction Reports and Analysis Centre by John Walker Consulting Services, September.

Walker, J. 1997, 'Estimates of the costs of crime in Australia in 1996' in *Trends and Issues in Crime and Criminal Justice*, No. 72, Australian Institute of Criminology, Canberra.

Walker, N. 1991, *Why Punish?*, Oxford University Press, Oxford.

Walker, V. 2003, 'Customs robbery "inside job"', *The Australian*, 10 September, http://www.theaustralian.news.com.au/printpage/0,5942,7222940,00.html.

Waller, L. & Williams, C.R. 1997, *Criminal Law: Text and Cases*, 8th edn, Butterworths, Sydney.

Warton, A. 1999, 'Electronic benefit transfer fraud: The challenge for federal law enforcement', *Platypus Magazine: The Journal of the Australian Federal Police*, vol. 65, December, pp.38–44.

Waye, V. 2003, 'Judicial fact-finding: Trial by Judge alone in serious criminal cases', *Melbourne University Law Review*, vol. 27, no. 2, pp.423–57.

Weisburd, D., Wheeler, S. & Waring, E. 1991, *Crimes of the Middle Class: White-collar Offenders in the Federal Courts*, Yale University Press, New Haven.

Western Australian Internet Association 1997, Code of Conduct, version 1.03, April 30. At, http://www.waia.asn.au.

Western Australian Internet Association 2002, *Spam Code of Conduct, version 1.28*, August 27. At, http://www.waia.asn.au/info/spamcode.shtml.

Williams, A. 2002, 'Crime and misconduct in the accounting profession', in *Crime in the Professions*, ed. R.G. Smith, Ashgate, Aldershot, pp.55–66.

Williams, C.R. 1999a, *Property Offences*, 3rd edn, LBC Information Services, Sydney.

Williams, C.R. 1999b, 'The shifting meaning of dishonesty', *Criminal Law Journal*, vol. 23, pp.275–284.

Willox, N.A. & Regan, T. M. 2002, 'Identity fraud: Providing a solution', *Journal of Economic Crime Management*, vol. 1, no. 1, Summer. At, http://www.jecm.org/02_vol1_issue1_art1.pdf.

Wolverton, T. & Gilbert, A. 2002, 'Fee fumble frustrates eBay users', *ZDNet Australia*, 19 August. At, http://www.zdnet.com.au/newstech/ebusiness/ story/0,2000024981,20267496-1,00.htm.

Wood, L. 2002, 'Class action filed against Harris Scarfe directors', *Age*, 31 July. At, http://www.theage.com.au/text/articles/2002/07/30/1027926885796.html.

Worldwide Electronic Commerce Fraud Prevention Network 2001a, *Fraud Test*. At, http://www.merchantfraudsquad.com/pages/test.html.

Worldwide Electronic Commerce Fraud Prevention Network 2001b, *Shop Safely*. At, http://www.merchantfraudsquad.com/pages/shopsafe.html.

Yellow Pages 2003, *E-Business Report: The Online Experience of Small and Medium Entrprises,* Yellow Pages Business Index. At, http://www.sensis.com.au/ Internet/static_files/YellowPages_EBusinessReport_July03.pdf.

Yellow Pages 2001, *E-Commerce and Computer Technology, Special Report: Survey of Computer Technology and E-Commerce in Australian Small and Medium Businesses*, Yellow Pages Business Index – Small and Medium Enterprises. At, http://www.sensis.com.au/Internet/small_business/ypbi/ smeiypbisr_023. pdf;jse .

Yellow Pages 2002, *E-Business Report: The Online Experience of Small and Medium Enterprises*, Yellow Pages Business Index – Small and Medium Enterprises. At, http://www.sensis.com.au/Internet/static_files/smeiypbibi_jul02.pdf;jsession.

Zervos, K. 1992, 'Responding to fraud in the 1990s', in *Complex Commercial Fraud* ed. P.N. Grabosky, AIC Conference Proceedings No. 10, Australian Institute of Criminology, Canberra, pp.199–209.

Zinn, C. 2000, 'Australian radiologists face prosecution for fraud', *British Medical Journal*, vol. 320, p.140.