DRUGS AND CRIME PREVENTION COMMITTEE

INQUIRY INTO FRAUD AND ELECTRONIC COMMERCE

DISCUSSION PAPER

PARLIAMENT OF VICTORIA

DRUGS AND CRIME PREVENTION COMMITTEE

INQUIRY INTO FRAUD AND ELECTRONIC COMMERCE:

EMERGING TRENDS AND BEST PRACTICE RESPONSES

Discussion Paper

October 2002

by Authority
Government Printer for the State of Victoria

Submissions are invited

The Committee welcomes written submissions in response to the issues raised in this Discussion Paper or on any matter related to the Terms of Reference of the Inquiry.

To assist interested parties in making submissions a number of questions have been posed throughout the Discussion Paper.

Details of how to make a Submission are included in the Insert. The Committee requires all submissions to be signed hard copy originals but would also appreciate an electronic copy.

Submissions should be sent by 30 January 2003 to:

Inquiry into Fraud and Electronic Commerce

The 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

The Discussion Paper was prepared by the Drugs and Crime Prevention Committee.

Drugs and Crime Prevention Committee
Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses – Discussion Paper
DCPC, Parliament of Victoria

ISBN: 0-7311-5292-1

The 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

Members

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 Peter Johnston
Senior Legal Research Officer
(Inquiry into the Use of Amphetamines and 'Party Drugs')

Ms Michelle Heane
Office Manager

Consultants, Inquiry into Fraud and Electronic Commerce

Dr Russell G. Smith
Deputy Director of Research
Australian Institute of Criminology

Mr Stuart Candy
Research Analyst
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 1968*, as amended.

Parliamentary Committees Act 1968 (Vic)

Section 4 EF.

> *To inquire into, consider and report to the Parliament on any proposal, matter or thing concerned with the illicit use of drugs (including the manufacture, supply or distribution of drugs for such use) or the level or causes of crime or violent behaviour, if the Committee is required or permitted so to do by or under this Act.*

Terms of Reference

Received from the Legislative Assembly on Wednesday 28 November 2001.

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.

Contents

List of Tables and Figures

Tables

Figures

page vii

Acknowledgments

This Discussion Paper 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, P.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 Jessica Marshall, formerly Research Assistant at the Australian Institute of Criminology.

Statistical information in Appendix E was provided by Victoria Police Statistical Services Division, Mr Michael Nieuwesteeg.

Library services were provided by the Australian Institute of Criminology's J. V. Barry Memorial Library (Mr John Myrtle and Ms Dita Kruze), the Victorian Office of the Correctional Services Commissioner's Resource Centre (Mr Malcolm Feiner), and the Parliament of Victoria Library (Ms Debra Reeves).

Mr Andrew Touhy from KPMG has given extremely informative briefings to the Committee.

Mignon Turpin has assisted the Committee in editing the Discussion Paper and Chris Watson from Zapwhizz.com.au has designed and laid out the contents of the report.

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. 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 while harmonising with measures implemented in other places in response to these global concerns.

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.

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). Consequently, 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, 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 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 an educated 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

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, breach of environmental protection laws, consumer protection offences relating to deceptive practices and the sale of dangerous or unhealthy products, infringement 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 Discussion Paper focuses on financial crimes perpetrated by individuals, as opposed to corporations, particularly financial crime involving the technologies of electronic commerce.

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 (see Chapter 6).

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 discussion. 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 we face the issue of fraud in the new

context of electronic commerce, 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 Discussion Paper 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 the discussion.

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 Discussion Paper, 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 6.

The focus of the present discussion 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 discussion 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 concerns and challenges presented in this Discussion Paper 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 cooperation between stakeholders. This means coordination and

cooperation 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.

Sources of information

The purpose of this Discussion Paper is to review current knowledge with respect to the issues raised by the Terms of Reference and to identify questions that key stakeholders and members of the community can answer so as to inform the Committee and the Parliament of Victoria and to serve as a foundation for its final report.

The research draws upon and integrates existing sources of information on the issue including statistical studies, surveys, prior academic and business reviews, information from government agencies, legislation, published police and judicial materials, and 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 Discussion Paper 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 Discussion Paper has not 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 in Victoria.

In addition, this Discussion Paper has drawn upon material received by the Committee prior to 30 August 2002 in response to its public call for submissions. Appendix A sets out details of those who made submissions in response to the Committee's invitation, and Appendix B sets out those who gave evidence before the Committee during the period of the reference thus far.

Conclusion

As is apparent from the preceding discussion, this Inquiry raises issues of far-reaching effect. The principal focus of this Discussion Paper is on the problems of fraud and financial crime involving electronic commerce as they affect Victoria, although responses will draw upon initiatives used elsewhere that may most effectively be adopted for use in Victoria. In addition, the Discussion Paper 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. This should not, however, deter policy-makers from seeking out appropriate and effective solutions, some of which may have existed for many years, others of which are yet to be devised.

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 the 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 focusing 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:

- A supply of motivated offenders,
- The availability of suitable targets, and
- 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 easily distinguishable on the surface from its illegitimate or illegal counterpart.

Greed

On occasions, however, fraud is committed by determined groups of organised individuals motivated solely by financial gain. One submission 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. It was thought 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.

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, 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[1] 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*, unreported decision of the Victorian County Court, 24 June 1993 ,Mullaly J; see the discussion of this case in Brown 1998).

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.

Financial strain

Financial strain caused through problem gambling is an area of concern that has recently been highlighted in the terrestrial and online worlds (Duffield & Grabosky 2001). The cost and addictive properties of illicit drugs may also contribute to financial stress on the part of those individuals who indulge in them. 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

1 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).

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.

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 neutralisations 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 to have a misanthropic view of human nature and assumed that others are as scheming and dishonest as they are. There is no doubt that generating a dislike and lack of respect for victims 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 becomes 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 (see the discussion of sentencing below in Chapter 6, under 'Criminal Justice System'.). 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 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 whether directly or 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 charge governments for goods or services which are not in fact provided (see Mills 1999).

The scale of such conduct ranges 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. 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.

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.

In Victoria, Ministerial Direction 10.1 made under the *Financial Management Act 1994* (Vic) requires accountable officers to ensure that:

> … all cases of suspected or actual theft, arson, irregularity or fraud under the control of the department are notified to the relevant Minister and the Auditor-General.

The Committee received a submission stating that the level of awareness of this requirement within departments in Victoria is poor and that cases have not always been notified to the Auditor-General. It was also suggested that the notification requirement be extended to all public sector agencies, including local government.[2] If this were to happen, the obvious potential difficulty is that the Auditor-General may require additional resources in order to investigate all the cases notified. Under the Audit (Further Amendment) Bill 2001 (Vic), the Auditor-General would be given a specific power to examine matters relating to waste, probity or lack of financial prudence in the public sector, unlike the present implied authority only.[3]

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,

2 Submission from J.W. Cameron, Auditor-General Victoria, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 13 August 2002.

3 ibid.

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.[4] Nevertheless, some areas of concern have been identified in Victoria. One submission received by the Committee 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.[5]

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 percent had formal fraud reporting systems, and only 35 per cent of respondents had carried out a fraud risk assessment.[6] A submission to the Drugs and Crime Prevention Committee relating to fraud in one TAFE Institute made allegations of sales tax fraud and improper use of government facilities.[7]

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 $1.8 million and $2.0 million for all departments and agencies. The bulk of cases related to claims under $5,000, as shown in Table 2.1.

4 ibid.

5 ibid.

6 ibid.

7 Submission from G. and M. Griffiths to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 8 July 2002.

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

Value of Fraud	Incidence
> A$1 m	1
A$50,000 - $100,000	1
A$10,000 - $20,000	5
A$1,000 - $5,000	12
< A$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, 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.

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 1996 there were 2.17 million professionals, according to the Australian Standard Classification of Occupations published by the Australian Bureau of Statistics (1997a). Employed professionals made up 17.1 per cent of the total Australian labour force while associate professionals made up 11.3 per cent. Together they comprised 28.4 per cent of the 8.4 million Australians aged 15 years and over in the employed labour force in 1996. Of the total number of professionals and non-professionals, 53 per cent were male (Australian Bureau of Statistics 1996a).

In Victoria in 1996 there were 335,123 professionals and 215,100 associate professionals, which together constituted 25 per cent of all professionals and associate professionals in Australia. Fifty-three per cent of Victorian professionals and associate professionals were male (Australian Bureau of Statistics 1996a).

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, p.55).

Electronic communications technologies, such as the Internet, are also enabling consumers of professional services to be better informed about matters that previously lay exclusively 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, p.89).

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 two 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 2002). 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 (for example, *McCabe v. British American Tobacco Australia Services Limited* [2002] VSC 73, Supreme Court of Victoria, 22 March 2002, *per* Eames J, subject to appeal; see also 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 ten 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. Paul John Crowley*, District Court of Queensland, 5 May 2000).

In the case of *R v. Fulton* (Supreme Court of Tasmania, 13 December 2001, Slicer J) 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.[8]

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 seven 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).

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 fraud and abuse in 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 in fact 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

8 Submission from J.W. Cameron, Auditor-General Victoria, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 13 August 2002.

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 – having a financial interest in, or having received an improper inducement from, the company selling the drug or appliance. 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, p.34). 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:

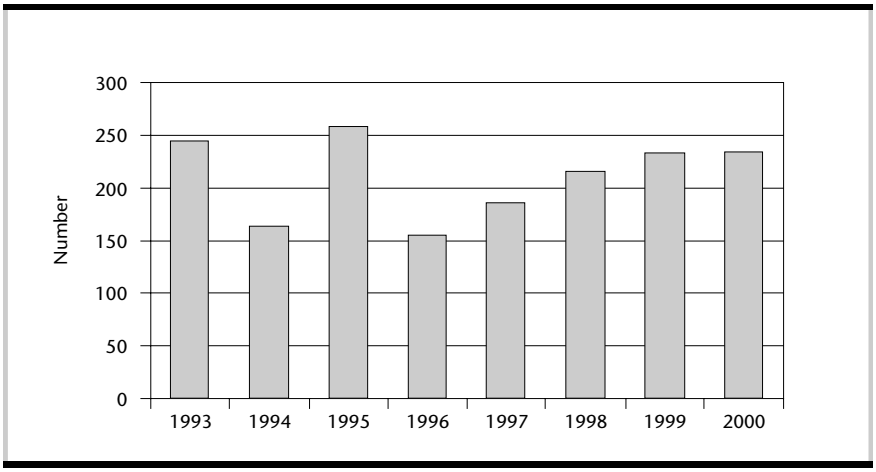
> … abuse of trust by having unprotected sexual intercourse with two current patients, by flagrantly defrauding Medicare, by misusing the doctor/patient relationship to borrow large sums of money from existing patients, and by encouraging an untrained person known by him to be HIV positive to assist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

Fraud in the corporate and business sector

In Australia, the Corporations Law is administered and enforced by the Australian Securities and Investments Commission (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 1993 and 2000 are presented in Figure 2.1.

Figure 2.1: ASIC investigations commenced, 1993–2000



Source: Australian Securities and Investments Commission (ASIC) 1993–2000, *Annual Reports 1993–2000*, 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).

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, the ICA claims that fraud still adds an extra $21 to the cost of every general insurance policy issued in Australia.[9] 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,

9 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.

for example, employees of a factory destroyed by arson are forced out of work and on to social security payments. The National Roads and Motorists Association (NRMA) estimated in 2001 that insurance fraud costs $820 per person or $2,660 per household in Australia annually (Gavan 2001).

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 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).

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 some 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 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, for example, *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

and exploited by fraudsters. Similarly, technology designed for use within the industry enabled the 'skimming' of account and personal information contained in the magnetic strip on the back of the credit card, thereby facilitating the creation of duplicate and counterfeit cards. One submission received by the Committee considered skimming to be a major concern resulting in significant losses to its business.[10]

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).

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 and 'Technological responses – User authentication' in Chapter 5 of this Discussion Paper). 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 (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

10 Anonymous submission received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

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.

An example of this kind of 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 desktop 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 $41,300 and reparation to the Commonwealth of Australia in the sum of $458,383.

Under Australian law the use of a false or alternate identity is not necessarily illegal and the use of an alias is common in entertainment and literary circles. Many women choose to use both their maiden and married names. There are, however, laws against using documents with intent to defraud. In addition, in an attempt to prevent large-scale money laundering the *Financial Transaction Reports Act 1988* (Cth) introduced a requirement for cash dealers (which includes many of the major financial institutions) to identify all signatories to accounts. The Act also made it an offence to open or to operate an account in a false name. To support this regime a process was established whereby numeric values were assigned to a defined group of documents – although none of them are officially considered to be adequate forms of identification in their own right. The 100-Point system, as it is known, provides for cash dealers to accept a combination of these documents as evidence of a person's identity unless there are obvious discrepancies. The increasing availability of technology that can be used to falsify documents, which to the average person appear to be genuine, has exposed a major – albeit unforeseeable – flaw in the 100-Point scheme. There has been a disturbing increase in identity-related fraud in recent years and financial institutions are now seeking to quantify losses from this particular type of fraud more accurately (see Chapman & Smith 2001).

In one submission received by the Committee, reference was made to trials being conducted in Victoria between financial institutions, the Office of Births, Deaths and Marriages and VicRoads, to verify documents tendered as proof of identity to financial institutions. It was found that approximately 18 per cent of birth certificates tendered did not correspond with information held by the Office of Births, Deaths and Marriages.[11] In a comparable trial conducted in New South Wales, where the Registrar of Births, Deaths and Marriages checked birth certificates used with Westpac to open bank accounts, it was found that 13 per cent of birth certificates presented were not an exact match with the records held by the issuing authority.

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 submission received by the Committee noted an emerging problem of home loan applications being made on the basis of false valuation information. It was argued that creating a central database of home valuation information, as some other states have done, would help to reduce this problem in Victoria.[12]

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 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.

11 Ibid.

12 Ibid.

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.[13]

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

Refund fraud

One area of concern identified in a submission to the Committee was refund fraud.[14] 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, p.30).

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, p.65).

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. Other offenders use proof of purchase receipts discarded by paying customers (Challinger 1996, p.33). In other cases, the offender takes an item off the shelves and directly presents it for refund (Sennewald & Christman 1992, p.18).

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, p.33).

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

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

14 Named confidential submission received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

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, p.30).

Fraud through the voiding of sales transactions occurs when an employee uses the 'void' function of a cash register dishonestly. The 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 customer (Hume 1996, p.26). 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, p.128). 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.

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. 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, p.2). 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 increasing the price or changing the identity of the vendor (Criminal Justice Commission, Queensland 1993, p.14). 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, p.3). 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, p.36). Its most direct impact on businesses occurs when a telemarketer contacts a business and persuades the manager into purchasing 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, p.140).

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.

The best way in which to avoid becoming a victim of telemarketing fraud is to be wary of cold-callers, irrespective of how persuasive they may seem (Grabosky & Smith 1998, p.147). Key indicators of a reputable telemarketing business include a willingness to send a written description of the products and a price list upon request, and to provide any information about the business, such as its location and history. Being able to verify key information is thus the basic requirement of telemarketing fraud prevention.

Abuse of credit facilities

Fraud perpetrated by suppliers of goods or services to small businesses can occur in a variety of ways, although each generally entails the abuse of credit facilities provided by the victim business. In its simplest form, a supplier establishes a line of credit with the victim, undertaking legitimate transactions in order to found a degree of trust, and then orders goods (often involving substantial sums), defaults on payment and disappears (Churchill 1997, pp.24–5). Various strategies have been employed to obtain credit and to disguise the identity of the defaulting business and its operators. 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, pp.1–2).

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, p.6).

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 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 (Australian Securities Commission 1996, p.1).

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, p.2). However, phoenix companies have been estimated to cost Australian businesses between $670 million and $1,300 million per year (Australian Securities Commission 1996, p.5). 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).

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, p.294). Because fraudsters often provide false business addresses and telephone numbers for trade referees, it is essential that referees be contacted and that independent information is obtained to verify the legitimacy of the contracting party (Churchill 1997, p.24). Conducting thorough checks on the financial standing of business clients to whom credit is extended is also obviously prudent.

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. As such, illicit funds can 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 three years Victoria Police has investigated a number of matters involving the authenticity of art works. In its submission, Victoria Police 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'. It was submitted that 'there is no specific legislation that governs the manufacture or sale of fraudulent art work, but it is generally covered by the offences of make and use false document under section 83A *Crimes Act 1958* (Vic)'.[15]

Fraud and 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, pp.105–29). Individual consumers also suffer the consequences of fraud committed against businesses through increased prices that are needed to compensate for losses sustained.

15 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

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.[16] 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 E-mail 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 US$20–40 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 approximately to 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).

One individual in Victoria was reported to have lost $400,000 through such a scam involving advance fee letters sent from West Africa.[17]

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).

16 Ibid.

17 Ibid.

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 youth.

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).

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, p.199, Table S2.5), it is to be expected that they would 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 are accordingly 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 one case investigated by the Victoria Police Major Fraud Group in 1996, a company accountant had used funds paid to him by the company for taxation liabilities. Instead the accountant used the funds for personal investment purposes relating to pre-paid funerals. Approximately $1.8 million had been defrauded in this and other ways. In Victoria, another company that made improper use of funds people paid for pre-paid funerals was convicted in July 1999 of failure to invest 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 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 percent of the victims were age 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 in fact 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 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.[18]

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 Minister for Consumer Affairs in Victoria recently drew attention to this problem, advising young consumers to 'get into the habit of reading the fine print when 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 provide 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 (see 'Criminal Justice System – Prosecution' in Chapter 6).

18 Ibid.

Conclusion

The ways in which people can act dishonestly are limited only by the 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.

Questions to Consider

What are the primary motivations for committing offences of dishonesty in Victoria, and what research evidence exists to document these?

In what ways, and to what extent, have professionals in Victoria committed offences of dishonesty?

Are professionals more likely to commit offences of dishonesty than people in other occupational groups?

To what extent is insurance fraud a problem in Victoria, and how have risks been addressed by the insurance industry?

To what extent are financial institutions in Victoria victimised by fraud and how are they responding to such risks?

To what extent are cases of suspected fraud notified to the Auditor-General, is the obligation to report cases of fraud to the Auditor-General adequate, and, if not, how could it be improved?

Are the steps being taken in both the public and private sectors to prevent and control fraud successful? In what ways could these steps be enhanced?

How can the nature and extent of fraud against individual consumers in Victoria be determined and who should be responsible for conducting such research?

In which areas are elderly Victorians more vulnerable to fraud than other age groups and why?

Is fraud against the elderly in Victoria more extensive than fraud perpetrated against other age groups? And if so, why?

3. The Extent of the Problem

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.[19] 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'.[20]

The best that we 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.

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.[21] 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

---

19 This point was stressed in an anonymous submission received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

20 Named confidential submission received by the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

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

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, not only will the potential benefits to victims be lost, but also the benefit to the wider community of deterrence. 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 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 survey of small businesses which included some crimes involving fraud (see Taylor forthcoming, and discussion below).

Official statistical sources of information

The nature and limitations of official statistics

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 bodies.

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.

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 coordinates the collection of data from official criminal justice agencies, the data collected at present are by no means complete, particularly with respect to offences of fraud and deception.

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, and if taken at face value can in fact 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 which appear as official statistics.

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

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 2000.

Table 3.1: Australian Federal Police number and value of economic crime cases referred for investigation, 1997–2000

Case type		1997-98	1998-99	1999-2000
Fraud	Number	360	308	312
	$000	125,970	104,410	207,269
Corporate, bankruptcy, intellectual property	Number	83	87	53
	$000	4,807	7,756	14,298
Computer/telecommunications	Number	163	250	69
	$000	229	3,215	1,101
Money laundering	Number	384	275	410
(Financial Transaction Reports Act 1988)	$000	101,578	70,751	60,358
Counterfeiting currency	Number	180	146	95
	$000	13,446	903	2,373
Environmental	Number	5	2	4
	$000	_	–	_
Other	Number	47	2,884	–
	$000	40,837	–	–
Total	Number	1,222	1,069	943
	$000	286,868	187,012	285,399

Source: Australian Federal Police 1997–2000, *Annual Reports*, Australian Federal Police, Canberra.

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 ($000)		Value of fraud cases ($)	
	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 eight per cent of the frauds reported were committed against fewer than ten 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 Classification of Offences (ASCO), 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 ASCO 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:

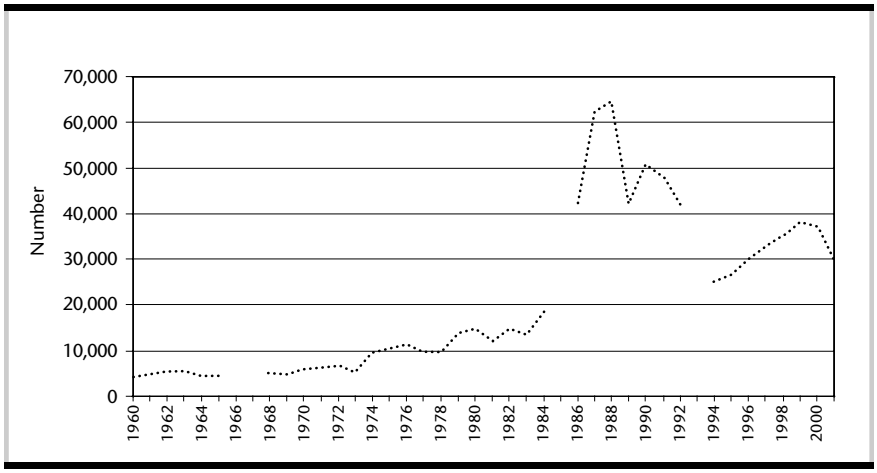
- offences of forgery and offences against currency only (Magistrates' Courts) (1960–1961);
- offences of embezzlement, false pretences, and fraudulent conversion (Higher Courts – County Court and Supreme Court) (1960–1962);
- offences of fraud, forgery and false pretences (Magistrates' Courts and Higher 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 Discussion Paper 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 2001 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.

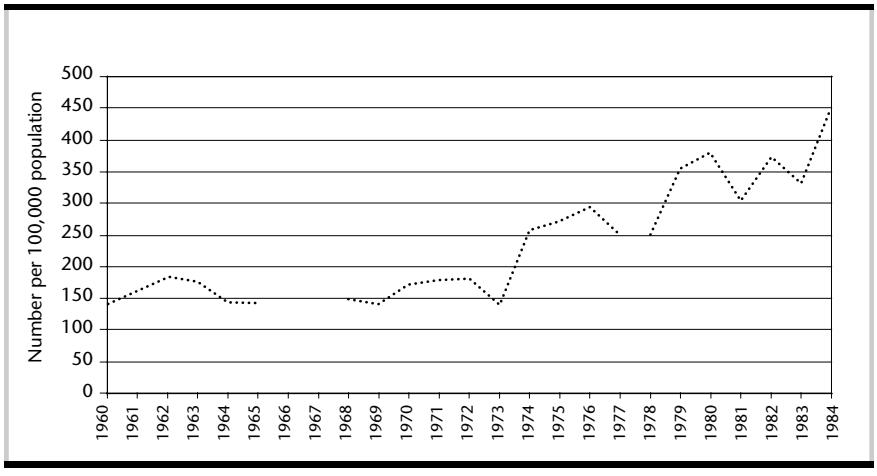
Figure 3.1: Number of Victorian fraud offences recorded by Police, 1960–2001



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.

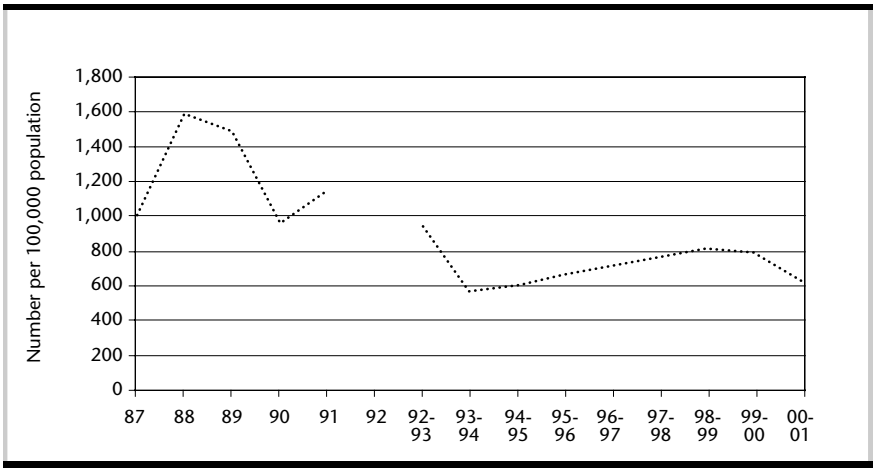
To understand the reasons for changes in the number of recorded offences it must be remembered that the population of Victoria has grown over time, making any increase in the raw number of offences reported not directly reflective of crime trends. Rates of deception offences per 100,000 of the Victorian 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, 1987–2001



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.

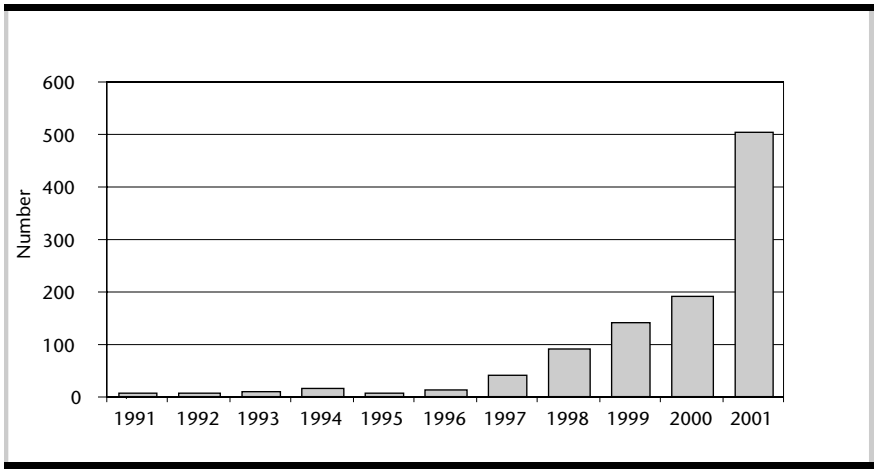
The large increase towards the end of the 1980s is due largely to the introduction of ANCO and the change in offence categories. In addition, this was a time of considerable change in the business world in Australia, which could have resulted in an increased incidence of dishonesty. One view is that 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.

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.

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, as is apparent in Figure 3.4 below.

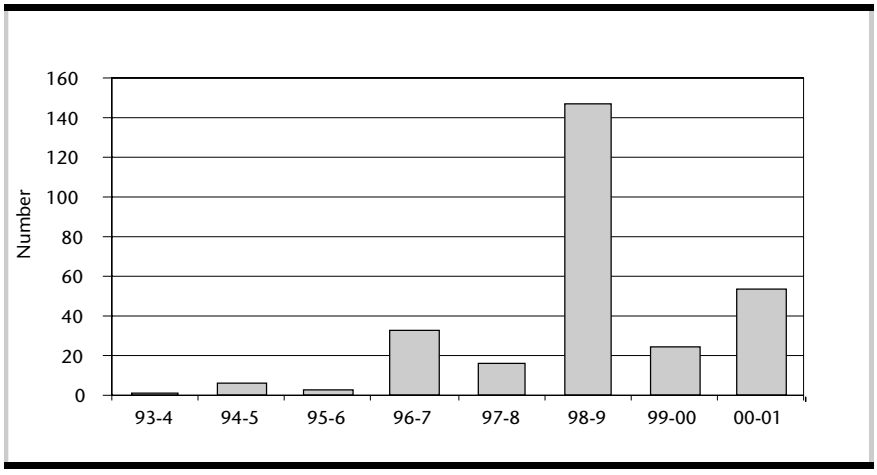
Figure 3.4: Electronic crime referrals received by the Australian Federal Police 1991–2001



Source: Australian Federal Police 1991–2001, *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 a substantial increase since 1993–94.

Figure 3.5: Computer-related offences recorded by Victoria Police 1993–94 to 2000–01



Source: Victoria Police 1960–2002, *Statistical Review of Crime 1993–2001*, 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'.

In previous years, when more specific information was provided, 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).

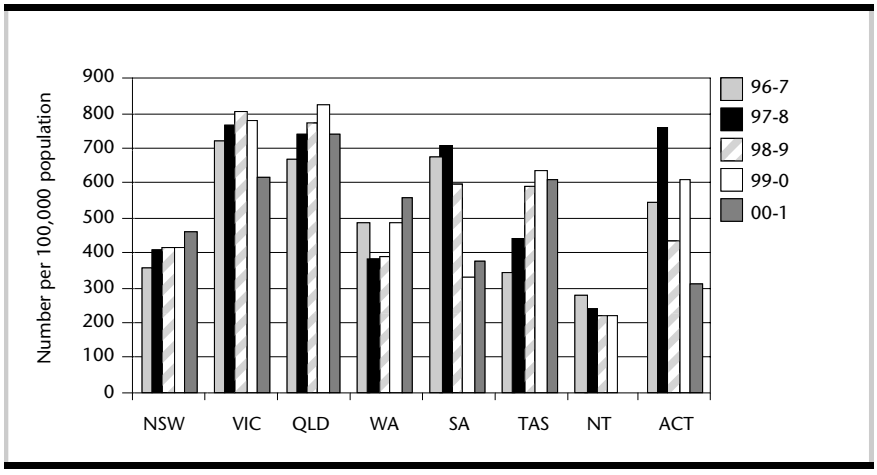
In 2000–01, the Legal Practice Board in Victoria received 95 claims representing over $4.2 million and conducted one prosecution against a conveyancer, resulting in a conviction and fine (Legal Practice Board 2001).

The Committee seeks information from these various professional bodies as to the nature and extent of complaints of dishonest activity investigated by them in recent years, particularly that which concerns electronic service delivery.

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 1995 to 1999, during which period Victoria experienced increasing rates of fraud offences reported to police. 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.

Figure 3.6: Fraud offences reported to Police for Australian jurisdictions 1996–2001 (Rates per 100,000 population)



Sources: NSW: NSW Bureau of Crime Statistics and Research 1997–2001; VIC: Victoria Police, Crime Statistics, 1996/97–2000/01; QLD: Queensland Police Service, Annual Statistical Review, 1996/97–2000/01; SA: South Australia Police, Statistical Review, 1996/97 –2000/01; WA: Western Australia Police Service, Annual Crime Statistics Report, 1996/97–2000/01; TAS: Annual Report of the Department of Police & Public Safety 1996/97–2000/01; 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 1996/97–1999/2000 (Note: NT data were unavailable for 2000–2001); ACT: Australian Federal Police, Annual Report on Policing in the Australian Capital Territory, 1996/97–2000/01.

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.

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. 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. 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 2000 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 ten 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. The latest international survey, conducted in October 1999, surveyed 11,000 senior executives in major organisations in 15 countries, 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 ten suffering more than 50 frauds. When combined, the single worst fraud suffered by all Australian respondents during the last 12 months totalled an estimated $20 million, with only $5 million of that having been recovered. Employees committed 82 per cent of serious frauds, with management committing one-third of these. Thirty-eight per cent of employee perpetrators of serious frauds were prosecuted and 28 per cent

were dismissed. In two 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.

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 Australian Institute of Criminology'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 5 full-time employees) comprised 56 per cent of the weighted sample, while small businesses (5 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		
	% 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 Australian Institute of Criminology coordinated 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 such as 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 six 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 thirty-nine 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 nine 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 we have seen. Between 1997 and 1999 the percentage of respondents who reported computer-related fraud rose from seven 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, a survey of 350 large Australian organisations was carried out by the Victoria Police and Deloitte Touche Tohmatsu (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 ten or more incidents. Twelve per cent reported theft of transaction information and six 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.

In the survey of computer crime and security conducted by the Office of Strategic Crime Assessments and the Victoria Police Computer Crime Investigation Squad (1997), four of the 11 government agencies surveyed reported misuse of their computer systems. Of these, five reported external forms of attack, that is, remote access to computer systems. The most frequently reported types of computer abuse reported by the government agencies surveyed related to damage or unauthorised access to data and programs or copying of data and programs.

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 2001, the Internet Fraud Complaint Center, organised by the United States Department of Justice and the Federal Bureau of Investigation, received 49,711 complaints relating to Internet fraud, 16,775 of which were referred to other authorities for further action. The average (median) monetary loss per referred complaint was US$435.00, with 43 per cent of complaints relating to auction fraud (Internet Fraud Complaint Center 2002).

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 200,000 complaints in 2001 (Federal Trade Commission 2002). This compares with 18,600 complaints in 1999 and 8,000 in 1998 (Department of Justice, United States 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 seven 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 was the fourth-highest contributor to complaints registered by the Internet Fraud Complaint Center in 2001, accounting for 0.5 per cent of complaints, behind the United States (93.4%), Canada (2.2%) and the United Kingdom (1.0%). Others in the top ten countries reporting Internet fraud were Japan, Germany, Singapore (0.2% each), Indonesia, New Zealand, and South Africa (0.1% each). The top countries from which perpetrators operated, of those cases where their location could be ascertained, were United States (87.6%), Nigeria (2.7%), Canada (2.5%), Romania, United Kingdom (both 0.9%), South Africa (0.5%), Australia (0.4%), Indonesia (0.3%), Togo (0.3%) and Russia (0.2%) (Internet Fraud Complaint Center 2002, pp.10, 14).

It must also be noted that Australians are represented not only as victims of fraud, but also as perpetrators. Procedures to allow inter-jurisdictional cooperation, including the facilitation by local authorities of foreign proceedings against Australian offenders, will probably need to be in place if we hope to secure the cooperation 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 ten types of Internet fraud recorded by the United States Internet Fraud Watch between 1999 and 2001 are shown in Table 3.7.

Table 3.7: Top Internet frauds, 1999–2001

Fraud type	1999 (%)	2000 (%)	2001 (%)
Online Auctions	87	78	70
General Merchandise Sales	7	10	9
Nigerian Money Offers	–	1	9
Computer Equipment/Soft.	1.3	1	2
Internet Access Services	2	3	2
Information Adult Services	0.2	1	2
Work-At-Home	0.9	3	2
Advance Fee Loans	0.2	2	1
Credit Card Offers	–	0.5	0.5
Business Opportunities/Franchises	–	–	0.5

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

Web sites were by far the most common way in which consumers encountered fraudulent Internet offers (90% in 1999 and 83% in 2001), although an increase occurred between 1999 and 2001 in the number of initial contacts made through E-mail (from 9% to 15% respectively). In some of the most frequently reported Internet frauds, many of the offers came by E-mail: 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.

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*.

The amount of money consumers lost to Internet fraud was also found to have increased, with the average loss per person rising from US$310 in 1999 to

US$518 in 2001. Losses overall were US$6,152,070 in 2001, almost double the total amount lost in 2000.

There were also differences in the methods of payment used by the victims of Internet fraud, 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*.

Although consumers are using their credit cards more online, money orders are still the most common way in which the victims of Internet fraud in the United States paid for their products or services. Some categories showed a large increase in credit cards for payments, while others such as Nigerian money offers continued 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. One submission received by the Committee from a business estimated the total cost of fraud to its businesses in Victoria in the financial year 2000–01 at $10 million including losses, staffing, resources and technology.[22] Another

22 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

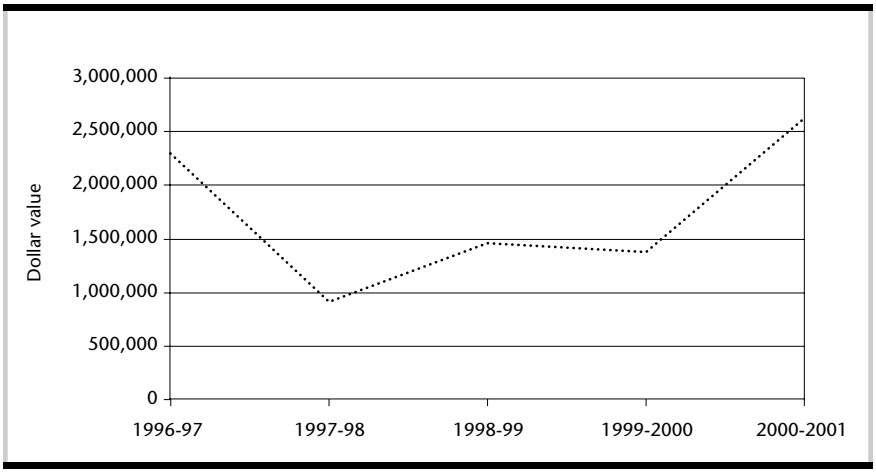
submission to the Committee referred to the indirect and unquantifiable losses associated with fraud and also noted how many financial institutions write off millions of dollars each year as 'bad debt' rather than recording this as criminal fraud.[5] This obviously makes any estimate of loss based on 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 2000–01



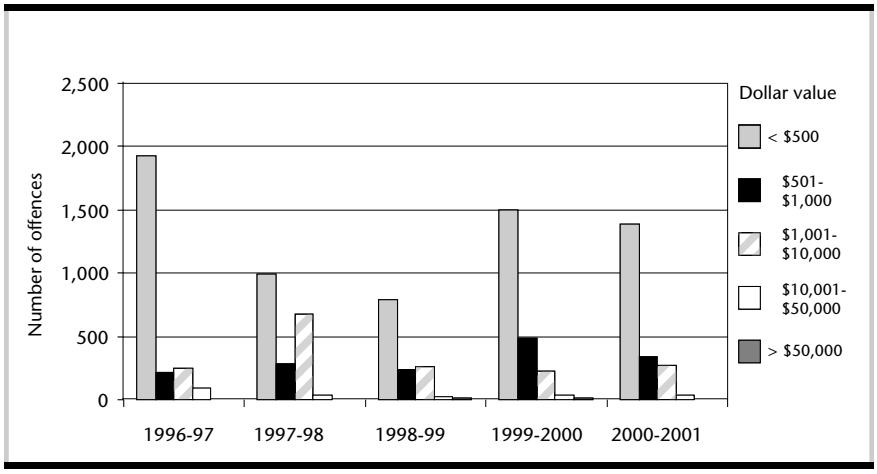
Source: Victoria Police 1960–2002, *Statistical Review of Crime,*Victoria Police, Melbourne.

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

5 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

year involved sums of less than $500 stolen or affected per offence reported. Although the total value involved has increased, this seems to have been due to a small increase in numbers of extremely high value offences, rather than in an increase in the number of smaller value offences (such as those less than $500).

Figure 3.8: Victorian deception offences – Dollar value stolen categories, 1996–97 to 2000–01



Source: Data provided by Statistical Services Department, Victoria Police 2002.

In 2000–01, published Victoria Police statistics (see Appendix D) showed that $1,371,957 was involved in deception offences reported to police, or just over $3,000 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 $2.2 million was lost to all fraud incidents in Victoria in 2000–01.

The problem with this estimate is its reliance on the reporting rate found by KPMG, as this survey concerned only large corporate entities. The Australian Institute of Criminology'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 $1.37 million would result in estimated total losses of between $11.4 million (using 12%) and $5.5 million (using 25%).

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), or approximately $200 million per year, or an average of $419,287 per organisation annually (Deakin University 1994).

The losses reported in the Australian Institute of Criminology'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 latest Australian *Fraud Survey* 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 2000–01, 29,753 fraud offences were reported to police in Victoria. Using KPMG's reporting rate of 62.6%, it can be estimated that 47,529 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 $290 million.

The problem with this estimate is that it is inaccurate to apply the multiplier of $6,113 per offence to all the reported police offences, as KPMG's respondents were confined to large organisations whereas police incidents relate to a wider variety of victims.

Calculations based on GDP

Walker estimated in 1996 that the financial and economic costs of crime amounted to at least 2.5 per cent of Gross Domestic Product (GDP) and that offences of fraud, forgery and false pretences accounted for approximately 28 per cent of the cost of all types of crime (Walker 1997).

In 2000–01, GDP in Australia was $641,370 million. In Victoria, Gross State Product for the same year was $164,383 million (Australian Bureau of Statistics 2002a, Table 9.3, p.126). Using the above percentages, the cost of offences of fraud, forgery and false pretences using Walker's formula would be $4,490 million for Australia and $1,151 million for Victoria.

The problem with this estimate is that it is based on the assumptions underlying Walker's calculation (see Walker 1995) and the assumption that the current percentages are the same as those he reported in 1996.

Clearly there is a need for a more sophisticated means of calculating fraud losses in Victoria. The Committee would welcome suggestions as to how this could be achieved. On the basis of the above figures (with their inherent weaknesses), fraud could cost up to $1.2 billion in Victoria annually at present.

Conclusion

Although there is a good deal of information currently available concerning the extent of fraud and computer-related crime, there are certain limitations that prevent the size of the problem from being ascertained 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 specific enough 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 approaching one billion dollars in Victoria alone per annum. More precise quantification must await more targeted and extensive research that will require the cooperation of public sector agencies and organisations in the private sector. This will need a commitment to conducting such research and to sharing information publicly, both within government and also within the private sector. Having a more precise understanding of the scale of the problem of fraud in Victoria could then be used to allocate fraud prevention resources and to develop new initiatives to control the problem.

Questions to Consider

In what ways can official police, courts and corrections statistics be improved to show the nature and extent of fraud in Victoria?

What research is needed to document the nature and extent of fraud victimisation perpetrated against businesses and individuals in Victoria, and who should be responsible for conducting such research?

What research is needed to document the nature and extent of fraud victimisation perpetrated by professionals in Victoria, and who should be responsible for conducting such research?

In what ways could officially recorded crime statistics be improved so as indicate the extent of fraud offences in Victoria and financial losses involved?

To what extent are Victorian offenders and victims involved in fraud offences dealt with by Commonwealth agencies?

4. Fraud Risks of Electronic Commerce

Introduction

Having examined the nature and extent of fraud and white-collar crime more generally, this chapter will focus upon the fraud risks inherent in the use of technologies of electronic commerce. Before considering some examples of dishonesty involving electronic trading, 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 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, that generate large volumes of credit card numbers which can then be used to pay for goods or services ordered online. The sole purpose of these credit card generator programs is to aid in finding particular credit card numbers that the program's user is not authorised to use but that online merchants will, nonetheless, accept. By generating a large enough group of card numbers that merchants will accept, participants in an online fraud scheme can make substantial fraudulent purchases of goods or services. They can also cause fraudulent billings for nonexistent goods or services, at the expense of the credit card company or the customers to whom the valid credit card numbers have been assigned (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).

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. Microsoft and Visa, for example, are developing a payment protocol called 'SET' (Secure Electronic Transactions) which uses public key encryption to protect data from being compromised. Digital signatures are also used to authenticate each of the parties involved (see 'Technological responses', Chapter 5). Credit card details are encrypted prior to transmission with the decryption keys being separately protected. Merchants receive payment by passing to their bank an encrypted message which originates with the cardholder permitting funds to be transferred from the credit card account to the merchant's account. The SET Protocol has undergone various revisions in recent years and its latest form, known as the 3-D Secure Protocol, is being implemented globally (Visa International 2001).

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 which 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 which 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.

Public key systems

In Australia, in accordance with the Federal Government's 'Project Gatekeeper' policy on electronic commerce, digital certificates have been issued by various agencies that permit secure electronic communications to be conducted between businesses and government agencies. 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 issued its own digital certificates to permit secure electronic communications between health service providers and itself over the Internet. In the private sector, two companies, Baltimore Certificates Pty Ltd and eSign, an Australian subsidiary of VeriSign, have been accredited to issue digital certificates to businesses seeking to transact business online with government agencies (Cant 2001).

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.

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 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 has yet to be announced.

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 onging 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 571 Internet Service Providers (ISPs) supplying Internet access services to 4.2 million active subscribers at the end of March 2002. Of these, there were 3.7 million household subscribers and 505,000 business and government subscribers. There were 1,234 million megabytes (Mbs) of data downloaded by Internet subscribers during the March quarter 2002, which is an average of 290 Mbs per subscriber. Of this, household subscribers downloaded 713 million Mbs (average of 191 Mbs each) and business and government subscribers downloaded 520 million Mbs (average of 1,010 Mbs each) (Australian Bureau of Statistics 2002b).

These quantities of data are put into perspective when one considers that one thousand pages of text is approximately one megabyte of data (1,234 million megabytes of data would correspond to some 1,234,000 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, over the six months to the end of March 2002, there were 212 ISPs at the end of the quarter, and 1,070,000 subscribers. In Victoria, 321 million Mbs of data were downloaded during the six months ending March 2002. In the same period, the number of ISPs decreased by 10 and subscribers decreased by 105,000. Data downloaded by Internet subscribers during the March quarter 2002 decreased by 10 million Mbs from the September quarter 2001 in Victoria (Australian Bureau of Statistics 2002b).

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. We have also seen the establishment of a number of online auction houses and the use of the Internet for the online share-trading and gambling sectors, 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 this 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 (NOIE 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 three years 2000–02, (from 17 per cent, to 26 per cent, to 41 per cent amongst small businesses, and from 28 per cent, to 49 per cent, to 61 per cent amongst their medium-sized counterparts) (Yellow Pages 2001, 2002).

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 2002 report revealed that online selling as a share of total sales activities has increased. Between 2001 and 2002 the proportion of online businesses that reported more than five per cent of their total sales orders online increased from 33 to 43 per cent. 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 42 per cent of respondents, up from 34 per cent in 2001 (Yellow Pages 2001, 2002).

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, 1994–2001

	1994	1995	1996	1997	1998	1999	2000	2001
Cheques*	3.7	3.9	3.9	3.7	3.7	3.2	3.1	2.8
Direct entry credits*	1.6	1.9	1.7	1.8	1.9	2.1	2.3	3.3
Direct entry debits*	0.3	0.4	0.4	0.4	0.6	0.8	0 9	1.3
ATM withdrawals**	40.7	38.8	41.6	39.2	42.9	41.9	48.4	64.0
EFTPOS**	20.6	29.1	35.5	39.2	44.5	48.6	52.0	57.5
Credit cards**	19.9	22.6	24.6	25.9	32.4	42.9	57.7	66.4

Note: * millions of items per day
** millions of items per month
Source: Australian Payments Clearing Association 2002, *Payment System Statistics*. http://www.apca.com.au/Paymentstatistics.html (visited 20 October 2002).

Table 4.2: Value of payment transactions, Australia 1994–2001

	1994	1995	1996	1997	1998	1999	2000	2001
Cheques*	24.8	23.4	24.3	24.9	14.6	12.3	9.7	7.6
Direct entry credits*	1.9	2.6	4.2	3.4	3.6	5.3	7.1	10.6
Direct entry debits*	1.3	1.2	1.6	1.6	2.4	4.0	3.9	8.2
ATM Withdrawals**	4.4	4.9	5.6	5.4	6.2	6.8	7.3	9.4
EFTPOS**	1.1	1.5	1.9	2.1	2.4	2.8	3.1	3.5
Credit cards**	1.8	2.0	2.3	2.5	3.6	4.3	6.4	7.5

Note: * A$ billions per day
** A$ billions per month
Source: Australian Payments Clearing Association 2002, *Payment System Statistics*. http://www.apca.com.au/Paymentstatistics.html (visited 20 October 2002).

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 late 1990s 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, BPay indicated that for the month of August 2002,

approximately 8 million electronic payments were made using its services, worth approximately $4 billion.[23]

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 terms of electronic funds transfers, the statistics compiled by the Australian Securities and Investments Commission (2000) on the operation of the Electronic Funds Transfer Code of Conduct in Australia show that there has been an increase from 42 to 64 complaints made under the Code per million transactions between 1998–99 and 1999–2000. In 1999–2000 there were 106,719 complaints out of 1,655,362,481 electronic transactions. This represents a very small proportion indeed, some 0.006 per cent. On this measure at least, it seems that electronic funds transfer systems operate in a secure and efficient manner.

Risks for government

Governments, because of the extensive use they make of computers, 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 cooperation between those involved in the procurement process (NSW Department of Public Works and Services 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).

23 Personal communication between Stuart Candy and Andrew Arnott, General Manager, BPay, 1 October 2002.

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 of which had already commenced implementation by 30 June 2002. 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. Already Electronic Benefits Transfer (EBT) is being used in Australia, and has been subject to abuse. Since 1997, EBT has been used by Centrelink for the delivery of social security benefits in several major Australian cities. The system operates on a national scale and assists in the electronic delivery of limited social security benefits in cases previously addressed using the traditional counter cheque.

A number of prosecutions have taken place in Australia in respect of internal fraud carried out by government employees fraudulently using the EBT computer system in December 1997 and January 1998. EBT cards were issued in fictitious names enabling the offenders to obtain cash at ATMs (Warton 1999).

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 E-mail (Dancer 2000, p.76).

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.

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.

Electronic funds transfer fraud

In the Australian Capital Territory in 1998, a financial consultant to the Department of Finance and Administration allegedly transferred $8.725 million electronically to private companies in which he held an interest, after

logging-on to the Department's computer network using another person's name and password. The individual in question was charged with defrauding the Commonwealth (*R v. Muir,* Australian Capital Territory Supreme Court, 25 September 2001). It was reported that $5.48 million of the missing funds has not yet been recovered by the police following an investigation (Campbell 1999).

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. Between 1 July 1997 and 30 June 1998, for example, 128,023 Medicare services amounting to $7,461,353 were processed by electronic funds transfer which, although a relatively small proportion of the 202.2 million Medicare services billed worth $6,334 million in the same year, is likely to increase considerably in the future.

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). The most recent 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, p.67).

Credit card fraud

Fraud relating to government credit cards is also a possibility. The Australian Civil Aviation Safety Authority recently 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 which 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, p.20). 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, p.30).

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. Their cases are currently before the courts. It was reported that the two men went on to sell some of these goods for sale 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 1998, p.43).

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 card holder has not contributed to the commission of the offence, the financial institution will 'charge-back' the amount debited to the card holder's account to the merchant who must then take remedial action against the offender – which is rarely possible.

One recent case of abuse of credit card information which was disclosed in an unencrypted E-mail message, involved 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 cell 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, namely, her card number, address and cell 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.

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 in the previous section 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.

Smart card fraud

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 include 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)

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.* E.D.N.Y., 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 undera strict definition of Internet fraud but they warrent 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 Internet Service Provider (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,* unreported decision of the NSW District Court, 27 March 1998; appeal to the NSW Criminal Court of 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. Making use of a false identity or using someone else's bank account are the usual. 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.[24]

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.

Risks for individuals

Identity-related fraud

One of the most common strategies 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 and 'Technological responses – User authentication' in Chapter 5).

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).

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

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 E-mail 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 Internet Service Provider and renting a telephone line from a carrier, each in a false name, provides an easy means of achieving anonymity. Free E-mail services offered by some Internet Service Providers 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 their true identity. These services may be used for legal reasons associated with enhancing privacy or for illegal reasons such as evading debts or police investigation of criminal activities. At present there are few 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 E-mail 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 cooperated 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. As previously mentioned, on 25 September 2001 a financial consultant formerly contracted to the Department of Finance and Administration was convicted of defrauding the Australian government by transferring A$8.7 million electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He was also able to obscure an audit through the use of other employees' log on names 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*, Australian Capital Territory Supreme Court, 25 September 2001).

The common feature in these cases is that the offenders used 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 www.paypai.com (using the letter 'i' instead of 'I'), so as to capture unwitting users' personal information (Sorkin 2001, p.18).

There is also no failsafe way of ascertaining the bona fides of claimed commercial affiliations on the Internet. Referees for organisations might in fact 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. As we have seen, even the endemic West African advance fee letter scams are now being conducted using E-mail, 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 cooperative 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 'Organisational responses – Internet sweeps' in Chapter 5).

Finally, the Internet is being used for various forms of unsolicited or bait advertising and illegal inertia selling techniques infringing local consumer protection legislation.[25] Although many of these scams seek to defraud consumers, they can just as easily target businesses and government agencies.

25 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.

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 (http://www.aba.gov.au/) is the body responsible for making and investigating complaints about prohibited Internet gambling content. Since 11 January 2002, only 11 such complaints have been received.[26] No Australian-hosted services have been found to be in breach of the legislation, and no cases have had to be referred to the Australian Federal Police for prosecution. Just four web sites offering prohibited gambling services, all based offshore, have been referred to Australian Internet Service Providers for inclusion in the filtering programs which they are required under the Interactive Gambling Industry Code of Conduct to provide to their clients (Internet Industry Association 2001).

The basis for the current arrangements is expressed in the Code as follows:

> 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).

26 Personal communication between Stuart Candy and Richard Fraser, Assistant Manager, Content Assessment, Australian Broadcasting Authority, 4 October 2002.

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 world-wide (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 recent report of the Internet Fraud Complaint Center (IFCC) in the United States estimated the daily number of transactions at 1.3 million. 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, p.5).

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 (IFCC 2001b, p.6). 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 (see Chapters 5 and 7) 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 'Smartcard 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.

According to one submission received by the Committee, actual dollar losses to the financial services industry caused through Internet banking have been minimal, with the majority attributable to identity-related fraud. It was noted, however, that keyboard logging programs (that are able to capture passwords and PINs) have been used to compromise Internet banking accounts.[27]

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 (ACCC 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 regularly being used 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

27 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

of fraudulent conduct involving the share market that have used the Internet to disseminate false information in order to attract investors, or to manipulate share pricess.

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 E-mail 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 E-mail contact to promote share investments (Australian Securities and Investments Commission 2001b).

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 E-mail 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 E-mail 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 ten 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 (2001a) 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, Stott J). In a separate prosecution, Wayne Loughnan

of Cawarral in central Queensland, who assisted Hourmouzis in the sharemarket 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 how business and government has responded to these challenges and where the most effective solutions lie.

Questions to Consider

To what extent is risk of fraud preventing individuals and organisations in Victoria from using the technologies of electronic commerce?

What specific fraud risks arise through the use of mobile commerce and messaging services?

In what ways can Victoria respond to the perceived threat of fraud so as to encourage the use of electronic commerce?

In what ways and to what extent does the new electronic procurement system affect fraud risk and monitoring in the Victorian public sector?

To what extent are the risks of fraud arising out of the use of electronic commerce described in this chapter present in Victoria? What other risks are present that have not been described?

5. Responses to the Problem

Introduction

Although the most obvious response to fraud is to report the matter to the police in order to have the offender convicted and punished, there are many other responses that some argue are more appropriate and cost-effective. This chapter identifies how public and private sector agencies have responded to the problem of fraud, and also considers various organisational and technological solutions that have been adopted. The chapter concludes by reviewing some of the key policy developments of recent years in relation to electronic commerce-related fraud.

Public sector responses

With the onset of fiscal constraints during the late 1970s, Australian governments have become increasingly sensitive to the risks of economic crime. 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).

Commonwealth funds are principally at risk in terms of benefits fraud and revenue fraud, although Victorian agencies can also be victimised from their internal staff as well as other members of the public, both within and outside the state.

It should also be recognised that, statistically, threats to information systems come disproportionately from within. As the Draft US National Strategy to Secure Cyberspace states:

> 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.

Financial management compliance framework

In Victoria, the Department of Treasury and Finance has established a Financial Management Compliance Framework to enhance awareness throughout the Victorian public sector of the provisions of the *Financial Management Act 1994* (Vic).

Fraudulent misconduct in the Victorian public sector can be investigated pursuant to 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 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.

In Victoria, monitoring of financial matters 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.[28] The Auditor-General has recently been involved in a review of the Financial Management Compliance Framework that is expected to be operational by 1 July 2003.[29] This will provide for effective corporate governance and risk management within the state's financial management framework.

In addition to this framework, various other pieces of legislation are relevant to the way in which fraud is dealt with in the Victorian public sector.

28 Submission from J.W. Cameron, Auditor-General Victoria, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 13 August 2002.

29 Ibid.

Other relevant Victorian legislation

The reporting of instances of wrongdoing across the public sector is facilitated by the recent *Whistleblowers Protection Act 2001* (Vic). Individual departments each have their own procedures for disclosures under this Act (see for instance Department of Justice, Victoria 2002 and Office of Public Employment 2002b).

In addition, Victorian government employees are required to comply with the Information Privacy Principles contained in the *Information Privacy Act 2000*, which came into effect on 1 September 2001. The Act sets out principles for the handling of personal information and creates binding obligations with respect to the collection, use and disclosure of personal information as well as setting access rights, although freedom of information legislation takes precedence. It applies exclusively to the Victorian public sector, as the *Privacy Act 1988* (Cth) covers information in the private sector.

The Victorian Government Purchasing Board (http://www.vgpb.vic.gov.au/) also establishes policies for government departments and offices to follow in relation to the purchase of goods and services, for example the policy on use of government credit cards which states:

> In recent years government issued credit cards have been linked to misuse including cash withdrawals and expenditure for private purposes. The new control environment provides for stricter oversight of use and clear consequences for public servants or statutory officers who misuse cards (Victorian Government Purchasing Board 2002, p.3).

The policy sets rules for use of these cards and a procedure for investigation of possible breaches.

Relevant Commonwealth responses

An important source of information and expertise for the investigation of financial crime is the Australian Transaction Reports and Analysis Centre (AUSTRAC). The work of the Centre was outlined in a submission to the Committee and the view was expressed that although police have had access to financial transactions reports information for more than 12 years, the full potential of AUSTRAC's financial intelligence has not been realised in the fight against fraud.[30]

AUSTRAC is Australia's anti-money-laundering regulator and specialist financial intelligence unit. 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

30 Submission from N. Jensen, Australian Transaction Reports and Analysis Centre (AUSTRAC) to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

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.

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 Australian Taxation Office (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.

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.

In the early 1990s another important strategy to control revenue fraud was introduced when the federal 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 tax file numbers to be compared with payment records held by the main Commonwealth Government departments providing benefits so that anomalies can be detected.

The Parallel Data-Matching Program permits anomalies in payments to be identified and targeted for further investigation, and 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 Parallel Data-Matching Program has not, however, been free from criticism, most of which has been directed at the covert way in which data-matching takes place and the fact 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). 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.

Proof of identity initiatives

Another key area for inter-agency cooperation 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. Cross-validation would enable 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.[31]

The Australian Bureau of Criminal Intelligence is also playing a leading role in the gathering of fraud-related information and intelligence with its National Fraud Desk. As part of this initiative, a pilot scheme has been established nationally to collate profiles of known identity fraud offenders to assist law enforcement agencies when investigating offences of this nature.[32]

In an attempt to reduce art fraud, Victoria Police have been involved in the Art Authentication Working Group, an initiative of the University of Melbourne and the Australian Commercial Galleries Association. A Working Party has been established in an attempt to develop policies and procedures to deal with questionable paintings in the Australian art market.[33] (see 'Fraud in the corporate and business sector – small and medium sized business' in Chapter 2, for more on art fraud).

31 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

32 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

33 Ibid

Private sector responses

In the private sector, as in the public sector, the best line of defence against white-collar crime is self-help. There is now a large industry that provides loss prevention and risk management services, 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.

Failure to have effective crime prevention and compliance systems in place may, in the future, result in corporations being subject to civil and criminal penalties, not to mention bad publicity, poor profitability and disruption to their operations.

One submission to the Committee recommended that the Victoria Police Major Fraud Group should be provided with additional resources to enable implementation of a fraud prevention program that would include training for business on aspects of fraud control, fraud detection, fraud awareness and effective reporting of fraud.[34] The Committee would welcome further submissions relating to the adequacy of funding for law enforcement and investigatory agencies involved in the investigation of serious and complex fraud matters.

Private fraud control services are by no means limited to prevention. Private organisations that find themselves the victims of fraud may either retain their own in-house investigators or engage specialised fraud investigators from the private sector. These private investigators may conduct an entire investigation, handing the matter over to the police for prosecution. This is a common response to fraud in the Australian insurance industry.

Where the victim lacks the resources to conduct its own investigation, prevailing constraints on the capacity of law enforcement agencies may require some form of hybrid agency. The increasing sophistication of many forms of fraud will require law enforcement agencies to engage the specialised skills of experts outside police ranks. Indeed, certain forms of fraud investigation are now routinely outsourced to private investigators. One imagines that as white-collar crime becomes increasingly refined, the role of private computer security professionals and forensic accountants will become greater, with law enforcement authorities hiring them for their specialised knowledge for individual cases.

It is important to recognise, however, that the functions and duties of private sector professionals differ from those of their counterparts in the public sector. Private sector professionals such as solicitors and accountants who act for corporations have a primary responsibility to their client, and the information

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

they collect and the advice they give is directed towards the needs of the client who is paying for their services. On the other hand, public sector law enforcement agencies have primary responsibility to the community at large in detecting, investigating, and prosecuting illegality. A tension thus exists between investigations that may assist the corporation in its future business affairs and investigations undertaken primarily for use in legal proceedings.

A good example of this tension is seen in the responsibilities of auditors examining corporate financial statements. Auditors have an important – but sometimes misunderstood – role to play in fraud control. If auditors detect material misstatements due to fraud they have a duty to report these in accordance with current legal requirements. Section 332 of the Corporations Law, for example, requires auditors to inform the Australian Securities and Investments Commission (ASIC) of any irregularities discovered in financial statements or any other contravention of the law. The extent to which these provisions require auditors to report evidence of fraud has been much debated. Moreover, the lack of clear guidelines has resulted in auditors being reluctant to report matters to ASIC or the police through fear of breaching confidentiality or giving rise to personal liability (see Krambia-Kapardis 2001).

It is not currently the function of auditors to seek out fraud. Rather, their role is to obtain a reasonable assurance about whether the financial statements prepared on behalf of the company are free from material misstatement. However, it should be remembered that many of the corporate collapses characterising what we have since come to describe as 'the excesses of the 1980s' included companies which had in fact complied with audit requirements. Blame should not be laid at the door of any one participant in corporate governance, as the stakeholders each have some measure of responsibility for ensuring that fraud is detected and dealt with, be they directors, managers, financial advisers, auditors, or those in public sector regulatory bodies. The risk is that unless there is close cooperation between all parties, each may believe it is another's primary responsibility to take action, with the result that no effective measures are taken at all.

In addition, as one submission received by the Committee noted, there is a need for information to be shared between organisations in the private sector in order to detect and prevent fraud. In particular, the sharing of fraud risk-related information between financial institutions may assist in preventing repeat victimisation and victimisation of other organisations by the same or other offenders using a similar *modus operandi*.[35]

35 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

Organisational responses

A wide range of strategies has been devised to deal with white-collar crime and fraud. Some of these strategies entail using the traditional legal measures of prosecution and punishment; and 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 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.

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, single-handedly led to its 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.

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.

Risk management

Organisations wishing to prevent fraud need to ensure that they have in place a range of risk management and fraud control measures. In the case of electronic commerce, however, obvious fraud control measures are sometimes overlooked 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).

In KPMG's *Global eFraud Survey* (2001), 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.

The need for effective risk management in electronic commerce is highlighted by 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 prior bad characters – 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 adequately when recruiting.

Corporate governance

Responsibility for the prevention of 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 crime and understand how that goal may be achieved, this will provide a foundation and model for their employees to follow.

However, achieving this aim presents difficulties in view of recent research revealing that most fraud is in fact perpetrated by managers. Such fraud may involve making purchases for personal use, misusing expense accounts or misappropriating funds (KPMG 1997, p.10). 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).

Another impediment to management taking a stance against white-collar crime may be a lack of detailed understanding by managers of how their organisations function, making it difficult for them to appreciate the risks that arise within their organisation. In an Ernst & Young survey of large organisations, less than one-third of the Australian respondents considered that their directors had a good overall understanding of their business for fraud prevention purposes (Ernst & Young 1998).

Where it has been proved that company directors have acted dishonestly or in breach of the Corporations Law, it is essential that they be prevented from repeating their illegal conduct at the same or some other corporation. Subsection (3) of s. 229 of the Corporations Law provides that persons convicted of certain offences are prohibited from managing a corporation, without the permission of a court, for five years from the date of their conviction or, if imprisoned, from the date of their release. One practical strategy to enhance compliance with these rules is the initiative taken by ASIC, which now maintains a public register of persons who have been disqualified from acting in the management of a company. This information is readily accessible to the public through information brokers as well as through the Internet (http://www.asic.gov.au/). At present the register does not include those disqualified because they are undischarged bankrupts or have been convicted of fraud, though it is intended that the register will be extended to cover these. By listing the names of disqualified persons on a public register, ASIC provides 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).

For some years now there has been robust debate on the extent to which regulatory agencies should present themselves as corporate police officers, responding to corporate illegality with a strong deterrent posture, as opposed to business facilitators seeking a cessation of the conduct in question, the recovery of ill-gotten gains and the preservation of assets. Clearly they have both roles, though the latter is probably more important.

Fraud control policies

Fraud control policies are widely being adopted in both the public and private sectors. Most government agencies 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.

Commonwealth

Many public sector agencies maintain policies designed to prevent and control economic crime. The Commonwealth *Fraud Control Guidelines*, for example, outline principles and standards of fraud control (Commonwealth Attorney-General's Department 2002). Although the guidelines relate only to Commonwealth 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 Commonwealth *Fraud Control Guidelines* define fraud against the Commonwealth 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 Commonwealth 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 Commonwealth 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 a Commonwealth 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 *Commonwealth Electoral Act 1918 (Cth.)*.

In 2000 the Australian National Audit Office (ANAO) (2000b) conducted a performance audit of fraud control arrangements in Commonwealth Australian Public Service (APS) agencies (2000b). The audit 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 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.

Australian Capital Territory

Significant advances have also been made in developing fraud control policies by various state and territory government departments. The ACT Government Service Fraud Prevention Unit, for example, 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 ten-point fraud risk management plan for NSW public sector agencies in 1994. This included principles of integrated macro policy, responsibility structure, fraud risk assessment, employee awareness,

customer and community awareness, fraud reporting systems, protected disclosures, external notification, investigation standards, and conduct and disciplinary standards (NSW Audit Office 1994). 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 eight 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.

Victoria

Victoria does not have a comparable fraud control policy that applies throughout the public sector, nor indeed is there a single fraud control policy that is used throughout the private sector. Instead, Standing Directions of the Minister for Finance made under the *Financial Management Act 1994* (Vic) require public sector managers to prepare and implement appropriate fraud management strategies to reduce the risk of fraud.[36] An Exposure Draft of a revised version of the Standing Directions was released in September 2002.

There has also been a recognition in recent times of the need to create an ethical environment in the public sector by educating public servants about the 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 such that their conduct should be governed by an overriding duty to act in the best interests of the community as a whole (see Mills 1999).

Private sector

In Australia, for example, the fraud victimisation survey conducted by Deakin University in 1994, found that 27 per cent of those surveyed had fraud prevention policies in place (Deakin University 1994). In November 1995, 48 per cent of the 123 Australian respondents to Ernst and Young's fraud survey had a fraud prevention policy in place and 51 per cent had conducted fraud reviews (Ernst & Young 1996). In Ernst and Young's subsequent fraud survey, almost three-quarters of the 84 Australian respondents indicated that their organisation had an explicit policy on fraud reporting (1998).

One-half of the respondents to KPMG's *Global eFraud Survey* (2001) had incident response procedures in place to deal with security breaches of their electronic commerce systems. Of those respondents who had procedures in place, 43 per cent had procedures that included computer forensic response guidelines to deal with wilful intrusions into their networks and to ensure proper gathering of evidence.

36 Submission from J.W. Cameron, Auditor-General Victoria, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 13 August 2002.

Although these policies are often capable of dealing with traditional forms of dishonesty, specific provisions in policies are also needed to deal with fraud involving electronic commerce. Both businesses and government agencies should establish guidelines, for example, on the allocation and use of passwords, on access to and use of the Internet for private purposes, personal use of E-mail, downloading government software, the use of copyright material, and reporting of inappropriate conduct.

In Australia in March 2000, the Office of the Federal Privacy Commissioner published guidelines on workplace E-mail, 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 generally require openness in 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).

Various standards have been designed to assist business and government in the creation and use of fraud control measures. Australian Standard AS 3806-98 Compliance Programs, for example, provides guidelines for both private and public sector organisations on the establishment, implementation and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes and in-house company standards, and to develop processes for continuous improvement in risk management (Standards Australia 1998). Several standards relating to information security management are already available (AS/NZS 17799, AS/NZS 7799.2, and HB 231:2000). At the time of writing, Standards Australia is also developing a Standard for Business Governance that it believes will be the first consensus-based document for corporate governance in the world (Standards Australia 2002). Among the issues to be addressed are anti-corruption and whistle blowing measures, which may prove useful in setting a benchmark for monitoring and dealing with electronic fraud perpetrated by insiders.

Codes of practice

Codes of practice may 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. The current

version of the Code, published by the Commissioner for Public Employment in 1995 under the *Public Sector Management and Employment Act 1998* (Vic) s. 37(1)(a), is on the point of being superseded (Office of Public Employment 2002a).

Like other codes of conduct, the new Code for employees in the Victorian public sector sets desired standards, but does not itself offer sanctions or investigation procedures for occasions when those standards are breached. It advises that official resources 'including computers, email, internet access and mobile phones' should be used for official purposes only, unless limited permission for private use has been given. Certain kinds of material are listed, 'fraudulent' material among them, that must not be sent by E-mail or other forms of electronic communication, or displayed or stored on computer. It is made clear that official information not already publicly available must not be used other than for official purposes without permission, and must not be released other than in accordance with the *Freedom of Information Act 1982* (Vic). Not surprisingly, employees are warned that '[y]ou must not take improper advantage of any information gained in the course of your employment'. Given that fraud offences by definition involve deception or dishonesty, it is to be expected that anyone engaged in or tempted toward such conduct would be fully aware that such actions are morally questionable, if not downright illegal. Therefore, any code of conduct shall invariably require supporting policy and procedure so as to facilitate deterrence, detection, and investigation consistently and effectively.

Advertising and marketing 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).

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) which was established in 1966 as the peak industry body for companies and individuals engaged in direct marketing in Australia, and 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, for example:

> 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 digitised 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 codes

The 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 Council 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 and, at the time of writing, a draft Code on privacy is awaiting ratification, and a new Code on cybercrime is in development.

The two state-based Internet industry bodies which 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 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' (WAIA 1997), and the South Australian Internet Association's Code of Ethics and Conduct states that all its members agree 'to act fairly, with integrity, conscientiously and honestly' (SAIA 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.

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 (4 megabits of text is roughly the length of a novel).

Only certain types of fraud, such as that perpetrated by mass unsolicited E-mail or 'spamming', could realistically be monitored. The WAIA 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 (WAIA 2002). A complaint-response system may suffer from the problem of vexatious complaints, necessitating investigation and thus a compliance burden. Further debate is clearly necessary in this area.

Online gambling codes

As previously mentioned (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 through the use of available technologies with the prevention of access by users to certain Internet content. 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.

Electronic commerce codes

In addition, in Australia, an Internet Code of Conduct has been created 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. The Australian Best Practice Model 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. The Best Practice Model 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.

In addition to this Best Practice Model, and as noted above, the Internet Industry Association is at present negotiating with law enforcement agencies to

produce a Cybercrime Code to enhance the level of cooperation between police and Internet service providers throughout Australia (Dearne 2002). This would help facilitate the investigation of cases relating to electronic commerce fraud and other cybercrimes in which the police require the assistance of ISPs.

Enforcement of codes

Non-compliance with codes of practice, however, is an area of continuing concern because there are usually few, if any, sanctions available. Occasionally consequences of non-compliance are provided for, such as in the *Fair Trading Act 1987* (NSW), section 74 of which provides that failure to comply with an industry code of practice may result in the agency 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 Australia in April 1998, Part IVB (ss. 51ACA to 51AE) was inserted in the *Trade Practices Act 1974* (Cth). 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. The first code to be mandated under Part IVB was the Franchising Code of Conduct, with effect from 1 July 1998. It is to be hoped that codes governing online misleading and deceptive practices will come within the jurisdiction of the Act in the future. (For discussion of consumer protection legislation, which lies behind the system of codes of conduct, see 'Substantive legislative environment', Chapter 6.)

The principal limitation with codes of practice as a regulatory mechanism is that 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).

Certification services

Some organisations are 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. (See, for example, the 'Which' webtrader site, http://whichwebtrader.which.net/webtrader/.)

The Council of Better Business Bureaus in the United States 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 do, in fact, 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 2001). 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.

Certification and endorsement services 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.

One of the main problems with endorsement and certification is the proliferation of services and the determination of appropriate standards. Already some 20 'Webseals' are in circulation in Australia. A comparative table is available which sets out their various attributes (see Cook 1999). 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 two 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).

Value restrictions

As an alternative to target hardening, it has been suggested that the risk of large-scale fraud and money laundering using Internet-based funds transfer systems could be minimised by placing limits on the size of transactions.

Mackrell (1996), for example, has suggested that stored value cards should have a modest limit placed on the maximum value that can be stored on them, especially if they are to be used for card-to-card transfers. There could also be a limit on the life of the cards, which would restrict their usefulness for hoarding and money laundering. Self-expiring cards have also been developed which automatically deteriorate after a certain period of time. In the case of online commerce, electronic restrictions could be placed on the value of transactions in order to avoid the possibility of large-scale fraud, although this may be seen as an unwarranted intrusion into freedom of electronic commerce.

Information services

Once policies have been established they need to be communicated and fully explained in order to prevent misunderstandings as to their meaning and effect. Often policies are established but not adequately implemented or publicised.

Providing educational material concerning fraud prevention and reporting procedures on internal agency web sites is also now widely used in the public sector. In the survey conducted by the Australian National Audit Office of Commonwealth fraud control arrangements, approximately 30 per cent of agencies used E-mail, and 35 per cent used their Intranet or public databases to disseminate fraud control information to staff (Australian National Audit Office 2000b, p.48).

In addition, direct E-mail fraud reporting facilities can be used, although if anonymity is required then telephone hotlines or even anonymous paper-based reporting may be preferable.

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. Many jurisdictions now have public interest disclosure legislation which aims to ensure that those who report illegal conduct are not disadvantaged by their conduct. In the case of computer-based illegality, as in other areas of crime, severe penalties could be imposed on individuals who engage in or attempt or conspire with others to carry out acts of reprisal against those who disclose illegality in the public interest. To date such remedies have rarely been used.

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.

An example of the way in which information and services directed against Internet fraud may reduce business vulnerability is the simple 'Fraud Test' to be found on the Worldwide Electronic Commerce Fraud Prevention Network (2001a) web site. 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?

The Worldwide Electronic Commerce Fraud Prevention Network (2001b) also offers practical advice on security and privacy protection for Internet purchases.

Similar advice is available from the Internet Fraud Complaint Center (2001a) on the following topics:

- Internet auction fraud;
- non-delivery of merchandise;
- credit card fraud;

- investment fraud;
- Nigerian letter scams; and
- business fraud.

The National Fraud Information Center, based in the United States, also provides advice through its Internet Fraud Watch web site (NFIC 2001). In another international initiative against consumer-related Internet fraud, a multi-lingual web site (http://www.econsumer.gov) was established to provide information on consumer protection legislation and other online fraud prevention measures, as well as a coordinated complaints mechanism. Countries participating are Australia, Canada, Denmark, Finland, Hungary, Mexico, New Zealand, Norway, South Korea, 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. Although initially introduced for the purposes of reducing consumer fraud on the Internet, many of these initiatives could be applied to the problem of Internet fraud in business and government contexts.

Internet sweeps

Consumer protection agencies now regularly conduct sweeps of the Internet in order to identify illegal practices and sites that contain misleading and deceptive information. The International Marketing Supervision Network (2002) (IMSN, http://www.imsnricc.org) 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 IMSN has conducted International Internet Sweep Days, led by the ACCC and incorporating the efforts of Victorian and other Australian agencies. They target dishonest online operations, responding to 'the growing number of fraudulent and deceptive scams emerging on the Internet'. 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) (ACCC 2001).

The first Sweep (aimed at get-rich-quick schemes) in 1997 located over 1,100 suspicious sites, which were sent advisory E-mails concerning their obligations under consumer protection laws. Two weeks later, approximately 25 per cent of those sites had been removed or altered (ACCC 1997). A similar sweep coordinated 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 cooperative efforts have proved to be 'a cost-effective compliance and public relations tool' (ACCC 2002b, p.5). However, the sweeps are also beginning to yield concrete outcomes. The ACCC reported

in September 2002 that as a 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 (ACCC 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.

Technological responses

In terms of target hardening, a wide range of technological solutions has been devised in order to reduce the risks of electronic fraud in both the public and private sectors. Some of the key areas to consider are as follows.

Hardware security

Organisations and individuals need to ensure that computer hardware is adequately secured by using appropriate firewalls and other technologies in order to prevent external forms of attack. In the 1999 KPMG fraud survey, poor physical security over computer equipment was found to be a common factor in allowing computer-related crime to occur (KPMG 1999).

User authentication

Human identification has been defined as 'the association of data with a particular human being' (Clarke 1994). Identity-related fraud (discussed earlier in Chapters 2 and 4) takes place where an offender defeats the user authentication strategies of a system, whatever they may be, and successfully identifies to the system 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. User authentication, or authentication of one's identity, is therefore crucial in preventing computer-based fraud.

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, pp.16–17). The integrity of identification systems based on tokens (identity cards and documents, passports etc.) is constantly being challenged and superseded. Identity-related fraud has thus become easier to perpetrate through the use of desktop publishing equipment (Smith 1999).

As noted in Chapter 2, it is when new users first have contact with an identification system that the system is most vulnerable to fraud (Willox & Regan 2002). To reduce the risk of fraud, new applicants to a system may be required to state various pieces of information about themselves, such as past telephone numbers and addresses. Arguably, the more information asked for, the less likely it is for an imposter to succeed in defeating the controls (p.2). This requires organisational and technological arrangements in place to 'gather sufficient control data', a particular challenge in the international setting (p.9).

The difficulty with such a proposal is that any background information capable of being secured for legitimate purposes can be located through the same avenues by those seeking to act illegally.

Willox and Regan describe the example of two September 11 hijackers who obtained Virginia state identification documents with false addresses, but using their real names (2002, p.3). Although the people involved in the attacks were said to have engaged extensively in various forms of identity-related fraud, it is difficult to see how the proposed model would have made any difference to the outcome in that specific case.

In all, the practice of user authentication is fraught with complexities, often with very high stakes attached to its integrity.

As businesses and government agencies continue to make use of electronic commerce and electronic procurement, the need to authenticate users' identities will become of critical importance. 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 Commonwealth Government formalise a process for working with other levels of government and industry to develop options for reducing and preventing identity fraud. A wide range of technological solutions has been devised to address the problems associated with user authentication, and it remains to be seen which solution, or combination of solutions, will be most effective.

Knowledge-based identification systems are also susceptible. As most online payment systems require the use of a PIN or password in order for users to gain access to personal computers, protection of such access information is the simplest crime prevention strategy available. Passwords are frequently misused and abused. It is possible to guess them, particularly if little thought has been given to their selection, or to use various forms of 'social engineering' to trick users into revealing them for subsequent improper use.

The use of brute computing force has also been used to break passwords. Cracking programs are available by which computers 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 use of massive computing resources (Denning 1998).

Users are best placed to protect themselves 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. Studies reveal, however, that between 20 and 70 per cent of people are negligent in using access code information (Sullivan 1987).

There are various ways of enhancing access security controls through technology. 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.

Challenge-response protocols may also be used as a means of carrying out user authentication. The server generates a random number that is sent to the card. In a public key system, the card digitally signs the number and returns it to the server. The server then validates the digital signature.

Alternatively, call-back devices may be used. After the user dials into a computer through a modem and gives his or her identity, 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, p.45).

A fourth authentication system not covered by the three categories noted above is based on location. 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 the system, which provides a safeguard against individuals pretending to be legitimate users who are located in a different physical location (Denning 1998).

One company, CyberLocator, produces a location signature sensor that uses signals transmitted by satellite to provide a location on earth at any given time. Late in 2001 a similar product known as VeriChip was launched by the American company Applied Digital Solutions, with the chief executive controversially remarking on the potential for use of the chips in monitoring the movements of foreigners entering the United States (Casey 2002).

Biometrics

Biometric user authentication is one of the three basic systems of identification noted in the preceding section, and at this time it is attracting great interest for the apparently higher level of integrity that it offers in comparison to the standard knowledge-based and token-based systems. In the future, biometric user authentication technologies will greatly enhance security, although privacy concerns will need to be addressed. Already there is a wide variety of systems being used which make use of an individual's unique physical properties. Common biometric identifiers today include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odours (Johnson 1996). Fingerprint identification systems are now being used to restrict access to keyboards and when using a computer mouse.

Although such systems achieve much higher levels of security than those relying on passwords, they are expensive to introduce and raise potential problems in terms of privacy and confidentiality of the personal data stored on computer networks. An initiative designed to reduce social security fraud in Toronto has been the enactment of legislation to enable welfare benefit recipients to use fingerprint authentication when dealing with the Ontario government in Canada. Detailed privacy protections are built into the legislation which includes requirements for all biometric data to be encrypted and for the original biometric to be destroyed after the encryption process has been completed (Cavoukian 1999).

In the wake of the September 11 attack on the United States, national security has been emphasised as a major priority in many countries. Among the measures being considered in some countries is the use of compulsory identity cards, which may or may not include a biometric identifier. It was reported in early 2002 that Hong Kong would begin issuing multi-use ID 'smart cards' to citizens from July 2003, replacing all 6.8 million existing ID cards by March 2007. They will contain basic biometric information such as thumb prints and a photograph, and will be capable of multiple functions including use as drivers' licences and library cards (Benitez 2002).

Such proposals face vocal opposition by advocates of privacy who raise the grave consequences of essential information being misused, such as that which 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:

> 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).

Biometrics, like other identification systems, is not impervious to misuse. In debate on what became the *Electronic Transactions (Victoria) Act 2000*, the views of a Canadian expert and key figure behind similar legislation passed in Ontario were noted as follows:

> 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).

It is important to bear in mind that there has never been an infallible identification system, and even a sophisticated biometric one must not be allowed to engender a false sense of security.

Digital signature security

Public key encryption systems represent one of the most effective ways of conducting electronic commerce transactions securely. Public key systems require that cryptographic key pairs be issued to individuals who are able to establish their identity to an appropriate degree of assurance by supplying multiple and independent sources of identification, such as when accounts are opened with a financial institution. Primary documentation (such as a passport or birth certificate) along with matching secondary documentation (such as a bank statement or car registration papers) are necessary to meet the requirements (see Chapter 6 for discussion of the 100-Point system of identification).

This, however, may prove to be one of the system's weakest points in terms of security. Already offenders have circumvented these systems by producing documents that have been forged or altered through the use of computerised desktop publishing equipment.

Once questions of identification have been resolved, issues would arise in relation to the manner in which keys or hardware tokens are given to users.

Standards for the storage and use of keys, perhaps requiring keys would also be needed to be used off-line or with a smart card which is able to process transactions.

The problem remains, however, that private key data or tokens themselves must be communicated to users. 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 which are stored on smart cards. Security precautions would need to be used to ensure that tokens are passed securely to users from the issuing authority.

Another area of risk concerns the generation of cryptographic keys. 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 may be 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 mechanisms such as personal identification numbers (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.

A significant and increasing proportion of public and private sector entities use electronic databases for maintaining sensitive and valuable data of some kind relating to their clients or users. Information security strategies may be formulated according to general principles adapted for the specific needs of any organisation seeking to improve the protection afforded to this valuable data (Arnold 2002).

One such model is predicated on a recognition that 'the all-knowing, all-seeing security system does not exist and cannot be built', so the one-layered 'egg shell' security approach – hard on the outside, soft on the inside – currently favoured by many entities is by definition inadequate (Arnold 2002, p.11). An alternative model is the 'Electronic Citadel', with its name and structure being drawn from an analogy to multi-layered military fortifications of the 18th and 19th centuries. Using electronic retail businesses as an example, it shows how customers' credit card numbers can be strategically encrypted and the keys periodically changed to ensure that vital information is presented in human readable form only when authorised and necessary.

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.

Document security

All systems of user authentication for electronic commerce transactions require users to prove their identity. Although the security of electronic communications may be greatly enhanced through the use of encryption, some of the greatest risks associated with electronic commerce arise as individuals seek to establish their identity when registering with authorities. Often identity documents are presented which are counterfeit or have been altered.

There are various solutions to the problem of counterfeit identification documentation fraud. 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 (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. This may not always solve the problem, however, as telephone answering services can be manipulated to support false employment or identity details.

Secondly, staff involved in validating documents need to be instructed as to the security features present on original documents, what original documents look like, and how forged documents appear.

Thirdly, modern security features should be incorporated on all documents used for identification purposes. 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. The use of these technologies makes counterfeiting extremely difficult.

Fraud detection software

If it is not possible to prevent online 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. A number of organisations are now providing software for use in the prevention of electronic fraud. Software has been developed to analyse user spending patterns so as to alert individuals to the presence of unauthorised transactions and also to analyse merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants (see Potter 2002). However, the success of such an approach depends upon the extent to which the software cannot be interfered with or modified.

One submission to the Committee also noted that such software, although regularly used by large financial institutions, is often beyond the means of

smaller businesses, which can become targets for criminal gangs aware of their greater vulnerability.[37]

Tracking and surveillance

It is also possible for technology to keep the activities of Internet users under surveillance. 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. Ideally, 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 (see 'Fraud control policies' and 'Codes of practice' discussion above, in this chapter). If agencies do permit staff to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law.

Where certain online activities have been prohibited, many government agencies now monitor the activities of their employees, sometimes covertly (such as through video surveillance or checking E-mail 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.

The use of computer software to monitor the business activities of government agencies also provides an effective means of detecting fraud and deterring individuals from acting illegally. The Australian Health Insurance Commission, for example, 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 addition, revenue authorities are able to make use of 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 Australian Taxation Office attributed more than $47 million in revenue assessed to its direct use of information

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

provided by the Australian Transaction Reports and Analysis Centre. 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).

Electronic commerce policy developments

In the early 1990s, the large Western democracies began introducing national policy frameworks designed to enhance electronic communication and to 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.

Initiatives of this kind have been taken up by other advanced countries 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 coordinate Commonwealth Government policy on electronic commerce, online services and the Internet. In relation to electronic commerce it 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 electronic crime (also known as cybercrime), of which electronic fraud is a subset. Subsequently an Electronic Crime Strategy was devised for 2001–03 and presented as 'the carefully considered views of law enforcement' on these issues. Its driving 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, 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, cooperative 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 proposed re-structure of the National Crime Authority and its replacement with an Australian Crime Commission has included an initiative that enables this body to now investigate cybercrimes. The Australian Crime Commission Establishment Bill 2002 (Cth) inserts in the definition of 'serious and organised crime' the offence of 'cybercrime', giving the Commission jurisdiction to handle offences of this nature. The Commission

will continue to have jurisdiction over 'fraud' as well as cybercrime if these fall within the general requirements of an offence that involves two or more offenders and substantial planning and or organisation; and that involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and that is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind and is an offence that is 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 cyber-crime 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.21–23).

In addition, the United States' 'National Strategy to Secure Cyberspace' sets out a range of measures to secure United States' information systems against deliberate, malicious disruption and to foster an increased national resiliency. Part of a possible disaster scenario noted in the document is that a terrorist group could:

> threaten to cripple e-commerce and credit card service for a week by using several hundred thousand stolen identities in millions of fraudulent transactions, if their list of demands are not met (United States, President's Critical Infrastructure Protection Board 2002, p.4).

In the United States, electronic networks and commerce have been highlighted as a site of vulnerability to future attacks, and their security from such attacks has become an urgent policy priority.

Conclusion

The responses to risks of fraud and electronic commerce have been diverse, entailing the provision of information to individuals and organisations on how to reduce and manage risks, as well as the development of new technological solutions that seek to make crimes of this nature more difficult to commit. Many policy responses have also sought to enhance the official reporting of fraud that has, traditionally, tended to remain a hidden problem. Raising awareness, however, can have its problems, as potential offenders could be inspired to try new techniques, or some solutions may bring with them counterproductive, unintended negative side-effects. Care is needed in devising appropriate responses to fraud to avoid such problems.

The next chapter will examine in more detail how the law, particularly legislative solutions, can be used to control fraud and the risks of electronic commerce. It is in this area that different jurisdictions and agencies need to work cooperatively, as fraud in the 21st century knows no borders.

Questions to Consider

To what extent do existing provisions relating to public sector fraud prevention, detection and prosecution in Victoria reflect best practice and trends in other jurisdictions?

How effective is the system at this time, and what emerging areas require closer attention?

What kind of innovations (such as fraud control policy, procedures or guidelines) implemented on a whole-of-government basis might improve matters in this area?

Is it appropriate for Victoria to have a standard Fraud Control Policy for all public sector agencies, and if so, what should it contain?

Should Victoria have a standard Fraud Control Policy that private sector organisations should adopt, and if so, what should it contain?

Should there be a central reporting agency in Victoria to receive all complaints relating to fraud and crimes involving electronic commerce? If so, how would this function and be administered?

To what extent does the Australian Transaction Reports and Analysis Centre (AUSTRAC) assist in the investigation, prosecution and prevention of fraud in Victoria, and how can its role in this regard be enhanced?

What role should be allocated to Internet Service Providers in the monitoring and response to fraudulent activity carried out by their clients?

What changes should be made to the regulatory arrangements of Australian Internet Service Providers?

What steps should be taken to improve the 100-Point system used for the identification of individuals who open accounts with financial institutions?

What measures are needed to prevent identity-related fraud when companies and businesses are registered and when individuals first register with government agencies?

How effective are the security arrangements governing public and private key systems, particularly concerning the registration and identification of individuals and the issue of keys?

6. Policy and Legislative Reform

Introduction

This chapter discusses the questions of policy and legislative reform by first considering the substantive laws that are relevant to the prosecution of fraud and electronic commerce in Victoria. It then examines a number of issues and problems arising in each stage of the criminal justice process – from reporting crimes, investigation and policing, gathering evidence from other jurisdictions, to prosecution, trial and 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. Fortunately, many reforms have already been undertaken and some effective solutions reached that have improved the operation of criminal justice agencies not only in cases of economic crime, but 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.

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 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).

The central dishonesty offences for Victoria 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*, unreported decision of the 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 dishonesty offences presented in Appendix C, however, the Victorian law in this area is by no means simple. Although Victorian laws concerning fraud and dishonesty largely follow the Model Criminal Code offences that have been enacted by the Commonwealth,

the Committee would welcome submissions giving views on whether the current law should be reformed and, if so, how this could be done to enhance its operation and further national harmonisation of criminal laws (as discussed below).

Arguably, reform in this area should be technology neutral rather than technology specific. The best example in this area would be the 'general' dishonesty or fraud offence, as advocated by Page (1997) and exemplified by s. 135.1 of the Model Criminal Code, discussed below.

There are, however, 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. Without further going into the detailed history of this controversy, it may be noted that this mental element is essentially no different for prosecution of a fraud perpetrated electronically than for dishonesty offences committed in more familiar contexts. It does, however, represent another layer of complexity in an area already distinguished by its evidentiary and jurisprudential complications.

Commonwealth fraud and dishonesty offences

As crime increases in the borderless online environment, the lack of uniformity of fraud law 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 help not only 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.

The problem of harmonising laws in Australia has been addressed by the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General. Already legislation has been enacted by the Commonwealth 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 Commonwealth Criminal Code 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* 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 ten 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 ten years' imprisonment for the first two, 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 UK Law Commission 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).

Proof of identity offences

There are also various regulatory pieces of Commonwealth legislation that set out offences for acting dishonestly when establishing one's identity.

The *Financial Transaction Reports Act 1988* (Cth), for example, regulates the manner in which identity must be established when accounts with financial institutions are created. 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 (s. 24 *Financial Transaction Reports Act 1988* (Cth)).

It is also an offence knowingly or recklessly to make a false or misleading statement in advising a financial institution of a change of name, which carries a maximum penalty of 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 Australia, the Financial Transaction Reports Regulations 1990 (Cth) establish the so-called 100-Point system in which proof of identity documents are assigned a value depending upon their level of security.

Under these regulations, 'primary documents', worth 70 points, 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 which 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, although 150 points may be required in order to establish one's identity for the most secure forms of electronic communications with the government in the future ('Project Gatekeeper').

Special provisions under the Financial Transaction Reports Regulations apply in relation to children, recent arrivals in Australia, non-residents and Aboriginal and Torres Strait Islander residents living in isolated areas (Regulations 6–9). The 100-Point system does not, however, provide a complete solution to the problem, as it is possible to submit documents that have been forged or altered through the use of computerised desktop publishing equipment.

In an attempt to deal with the problem of identity-related crime in the United States, specific legislation has been enacted. The Federal *Identity Theft and Assumption Deterrence Act* of 1998 (18 USC 1028) which became effective on 30 October 1998, makes identity theft a crime with maximum penalties of up to 15 years' imprisonment and a fine of US$250,000. It establishes that the person whose identity has been stolen is a victim who is able to seek restitution following a conviction. It also gives the Federal Trade Commission power to act as a clearinghouse for complaints, referrals, and resources for assistance for victims of identity theft. Some 47 American states now have some form of identity theft legislation, although the Federal Act is the most comprehensive. The Committee would welcome submissions on whether such a model would be appropriate for introduction in Victoria.

Computer crime

The provisions introduced by the *Crimes (Computers) Act 1988* (Vic), though far from exhaustive of the potential range of offences for computer criminals, are the most comprehensive of their kind in Australia. This Victorian legislation was described early last year as 'perhaps the most elaborate Australian example

of legislation aimed at computer fraud' (Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2001, p.87).

In addition to those provisions dealing with dishonesty (giving various dishonesty offences in the *Crimes Act* an extra-territorial reach; making the falsification of documents an offence; and enabling obtaining property by deception to cover deception of a computer or machine), the 1988 Act also put in place the summary offence of 'computer trespass' through the introduction of section 9A *Summary Offences Act 1966* (Vic). Case law has shown that conviction for unauthorised access under the existing section 9A is possible despite a defendant being an 'insider' with legitimate access to a restricted system in the course of their employment. In the Victorian Supreme Court case *Director of Public Prosecutions v. Murdoch* ([1993] 1 VR 406), Mr Justice Hayne concluded that a bank employee's use of his restricted access privileges to switch an ATM 'off-host', so as to overdraw his own account, was without lawful authority.

It can be seen from the statistics provided in Appendix F ('Computer offences') that charges under this section have been recorded in significantly higher numbers since about 1997. However, it appears that this section will soon give way to a new computer offence regime. The Crimes (Property Damage and Computer Offences) Bill 2002, recently introduced into the Victorian parliament, proposes to have this summary offence repealed and a comprehensive set of seven new computer offences put in the *Crimes Act* instead. If passed, the new Victorian legislation would expand the net of criminality to cover a range of computer-based activities not explicitly dealt with at present.

The proposed offences under the new Bill are as follows:

- Unauthorised access, modification or impairment with intent to commit a serious offence (*Crimes Act 1958* (Vic) proposed s.247B; corresponding to the Commonwealth Model Criminal Code s.4.2.4);
- Unauthorised modification of data to cause impairment (s.247C; MCC s.4.2.5);
- Unauthorised impairment of electronic communication (s.247D; MCC s.4.2.6);
- Possession of data with intent to commit a serious computer offence (s.247E; MCC s.4.2.7);
- Producing, supplying or obtaining data with intent to commit a serious computer offence (s.247F; MCC s.4.2.8);
- Unauthorised access to or modification of restricted data (s.247G; MCC proposed summary offence); and
- Unauthorised impairment of data held in a computer disk, credit card or other device (s.247H; MCC proposed summary offence).

The first three offences would be punishable by up to ten years' gaol, the next two by up to three years', and the last two by a maximum gaol term of two years.

The proposed legislation is nearly identical to the recommendations of the Model Criminal Code Officers' Committee of January 2001, and follows an agreement on Terrorism and Multi-jurisdictional Crime between the Prime Minister and state and territory leaders, which was struck in April 2002. Some of these could be used to prosecute fraud carried out through the misuse of computers, such as where a person gains access to a computer by using another person's password without authorisation.

The corresponding Model Criminal Code offences noted above were introduced in the Commonwealth by the *Cybercrime* Act *2001* (Cth), which was assented to on 1 October 2001 and commenced on 21 December 2001. This Act inserted a new Part 10.7 (Computer Offences) into the Commonwealth *Criminal Code Act 1995* (Cth) and largely follows the provisions of the Council of Europe's *Convention on Cybercrime* (discussed below). 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.

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

It is interesting to note that the Commonwealth *Cybercrime Act 2001*, in amending the Criminal Code, follows the international example of the European Convention on Cybercrime. The 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 October 2002, 30 of the 44 members of the Council, and all of the four non-member states involved in elaborating the document, had become signatories. However, only one country, Albania, had gone on to ratify 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 Model Criminal Code offences follow certain parts of the Convention, for instance the preparatory offences set out in sections 4.2.7 and 4.2.8. The offence 'unauthorised access with intent to commit an offence' (proposed *Crimes Act* s. 247B; MCC s. 4.2.4) goes well beyond the *Computer Misuse Act* 1990 (Eng) which was the original model. Thus, the Crimes (Property Damage and Computer Offences) Bill 2002 (Vic) follows closely developments at both the Commonwealth and international levels.

Mention should also be made of Part 4.3 of the Victorian Bill dealing with sabotage and cyber-terrorist offences. Following the shift in world politics that began with the September 11 attacks, it can be seen that possible terrorist activity oriented to information networks – though not a matter of fraud – has appeared on the agenda in both the public and private sectors (see 'Electronic commerce policy developments' in Chapter 5). The vulnerability of electronic commerce infrastructure to malevolent attacks of this nature must not be overlooked. If passed, the Bill would remedy this along with other lacunae in the existing law, also implementing penalties of unprecedented strictness for computer offences, to align them more closely with 'offline' crimes and community attitudes.

A further proposal in the area of computer crime before Parliament at the time of writing is the Crimes (Stalking and Family Violence) Bill. This bill would amend the *Crimes Act 1958* (Vic) to, among other things, make it an offence punishable by up to ten years' imprisonment to post false information about a person or to impersonate a person in a chat room (Keenan 2002). There is no reason why these forms of deception could not occur in a commercial context, or for financial reasons. The Committee would welcome submissions on the question of whether such activities are already adequately proscribed in existing law (including civil actions for defamation) or whether they should be explicitly criminalised.

One area of legislative concern raised in a submission to the Committee is the difficulty of prosecuting individuals who have in their possession equipment that is to be used for the commission of computer-related offences.[38] It was argued that, for example, currently the importation or possession of credit card skimming devices is not illegal. Hong Kong legislation was cited that permits individuals to be charged with possession of any article used for or in connection with the illegal manufacture of credit cards. However, problems arise where electronic devices have multiple purposes, some legitimate and some illegitimate, as it may be difficult to prove that the offender possessed the device for an illegal purpose. The Committee would welcome comments as to whether such a reform would be appropriate for Victoria.

In October 2002, Visa International paid for over 30 police officers from around Australia to attend a series of training sessions on dealing with credit card skimming (Fitzsimmons 2002). Such cooperation between public and private sectors to deal with a shared problem may become more common in future as the pressures of sophisticated crime encourage more concerted and innovative responses.

A related lacuna in the Victorian legislation is the absence of a criminal offence of possession of a counterfeit plastic card. Although it may be possible to prosecute this conduct under the offence of possession of a false document (s.

38 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

83A(5) *Crimes Act 1958* (Vic), it is arguable that a more specific offence ought to be enacted as it is often difficult to establish the requisite intent necessary to prove possession of a false document in these circumstances.[39] One submission received by the Committee considered that an offence should be enacted proscribing possession of counterfeit cards whether or not they are located at the offender's place of abode.[40]

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 (1999, p.112).

Specific measures have recently been implemented in Victoria to facilitate the confidence of consumers in taking their business online by addressing these concerns. 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

39 Ibid.
40 Ibid.

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-contact 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 s. 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 s. 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 comparatively 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.

A number of web sites exist that are specifically oriented to the end of assisting concerned Internet users to target online offenders, or to protect themselves, or both. Internet Fraud Watch (http://www.fraud.org/internet/intset.htm), Cyberangels (http://www.cyberangels.org/) and ScamBusters e-Zine (http://www.scambusters.org/) are among them. As for Australia, in October

2001 a web site, http://www.scamwatch.gov.au, was launched by consumer affairs agencies around the country to educate consumers about online fraud risks. These agencies, among them the (federal) Australian Competition and Consumer Commission (http://www.accc.gov.au) and Consumer Affairs Victoria (http://www.consumer.vic.gov.au) also offer their own resources on the issue). Other resources 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), ASIC's consumer watch site FIDO (http://www.fido.asic.gov.au); and the Department of Communications, Information Technology and the Arts (2002) , which also offers advice for online shoppers,.

In short, there is no dearth of advice being dispensed by government departments and offices; if anything, people seeking guidance in the area may suffer from information being disseminated through too many avenues. A related risk is that if too many entities are involved in the collection of data about online fraud incidents, statistics may be distorted through multiple or selective recording by different agencies.

At the international level, still further initiatives are under way. In 1999 the OECD completed and adopted *Guidelines for Consumer Protection in the Context of Electronic Commerce* (Organisation for Economic Cooperation and Development 1999). In April 2001, responding to the challenges of multinational Internet fraud, 13 countries unveiled *econsumer.gov* (http://www.econsumer.gov/english/about.htm), a joint effort to gather and share cross-border e-commerce complaints.

In view of the enormous challenges presented by online fraud against consumers, these cooperative ventures are a welcome development and, one hopes, a sign of things to come in this area. Global problems undoubtedly require global solutions.

It must be recognised, however, that significant difficulties may attend these efforts to coordinate consumer protection across jurisdictions, as there is room for genuine disagreement about how much 'protection' should be accorded to consumers. A situation that from one perspective could be regarded as unacceptable fraudulent behaviour might be construed quite differently from another ideological vantage point that sees the case as 'sharp business practice' or simply carelessness on the part of the aggrieved customer. The laws of countries, like the opinions of individuals, may legitimately vary when it comes to such matters. International offenders are likely to try to take advantage of such disagreements, seeking to operate from within jurisdictions where, for whatever reasons, consumer protection is less strictly maintained.

One particular difficulty in this area deserves mention. As we are now aware, and as this Discussion Paper seeks to illustrate, the tremendous potential provided by the technologies and infrastructure of electronic commerce can readily be turned to illegitimate ends too. The unfamiliarity of new Internet users with the traps and pitfalls of electronic commerce will probably lead to an escalation of numbers of fraud victims temporarily, as the uninitiated segment of the market comes online. Effective prevention requires that new users be aware of the dangers awaiting them in advance, but how best to raise awareness and encourage self-protection among new users without also driving away or slowing down the market? This is a major challenge.

Information privacy

The issue of information privacy overlaps with fraud or identity theft prevention. A sound legal basis for confidence in electronic commerce and information storage is evidently 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 imposters, 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 subsequently passed *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*. This 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 Hungary, Switzerland, Canada and the United States had been designated as having sufficient data protection legislation in place for EU members to safely send personal information there (European Commission 2002). 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 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). Both this question and the question of how well the legislation is working in the prevention of fraud are worthy of further attention.

The preamble to the Commonwealth *Privacy Act 1988* 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 Discussion Paper.

Criminal justice system

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.

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. It also aims to deter others in the community from offending by making an example of the individual in question. 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 such as doctors 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.

Arguably, fines are a better sanction for white-collar offenders as they permit reintegration to take place (see 'Sentencing' below).

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 personal 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.[41]

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.[42]

In responding to illegality surrounding electronic commerce, law enforcement agencies need specially trained units to handle investigations. In some cases, forensic accountants from the private sector may be engaged by police fraud squads to carry out investigations, or part thereof. In other cases, independent statutory anti-corruption agencies may take action and they too may need to develop expertise in this area. In New South Wales, for example, the Independent Commission Against Corruption developed Project Mercury, a strategy to deal with electronic corruption, and already a number of its investigations have involved cases of electronic fraud (Bell 2000).

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

42 Ibid.

Reporting

The first barrier to the 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.

It is also impossible to know precisely the extent of under-reporting of crimes committed in this way. Where individuals are aware that they have been victimised by white-collar criminals, the law requires, in certain circumstances, that they bring this fact to the attention of the police.

Subsection 1 of s. 316 *Crimes Act 1900* (NSW), for example, 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.

The question arises as to whether professionals should be under a duty to report fraud offences to law enforcement and or regulatory agencies. This could prove beneficial, although protection would need to be in place to guard against reporting for other than bona fide reasons and to ensure that reprisals cannot be taken against those who report matters. In addition, more resources may be required if mandatory reporting leads to a substantial increase in the number of complaints needing to be dealt with.

In a submission received by the Committee it was argued that financial institutions should be provided with an online system that would enable them to report fraud-related information directly to the police for both intelligence and investigatory purposes.[43] It was proposed that an 'input only' computer terminal be installed in financial institutions with direct access to the Law Enforcement Assistance Program (LEAP) maintained by Victoria Police. Once again, this would entail providing the police with additional resources to deal with the new source of information and security of data would need to be ensured. The Committee would welcome responses regarding the implementation of such an idea.

43 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

The latest KPMG fraud survey found nearly four out of every ten fraud offences were not reported to the police by the victim organisation (KPMG 2002, p.15), indicating that, despite the legal requirement, there are powerful reasons why individuals may not wish to report offences to the authorities. In a Deakin University survey of organisations in Victoria, reasons given for not reporting fraud to the police included a belief that the matter was not serious enough to warrant police attention; a fear of consumer backlash; bad publicity; inadequate evidence; and a reluctance to devote time and resources to prosecuting the matter (Deakin University 1994, pp.45–6).

In another submission to the Committee, a large corporation expressed its dissatisfaction with police investigations owing to a lack of resources or inability to deal with complex matters. The corporation had offered to assist in 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.[44]

On a more general level, increasing resources to law enforcement agencies would help to generate confidence in the ability of agencies to investigate and prosecute allegations of white-collar crime. At present, many cases that are reported simply cannot be investigated because law enforcement agencies are under-resourced, particularly for serious, complex, and time-consuming allegations involving fraud and deception.[45]

An additional impediment to the reporting of white-collar crime lies in the fear which 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. People with information about white-collar crimes, particularly large-scale fraud, should be encouraged to come forward and to report them 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 in fact unlawful and results in prosecution where it is detected.

The *Whistleblowers Protection Act 2001* (Vic) which has been in full effect since 1 January 2002, attempts to do just that, providing protection for '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

44 Named confidential submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

45 Ibid.

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). Earlier whistleblower protection statutes introduced in various Australian jurisdictions have had mixed results (see De Maria 1995), but as this protection is now available to Victorians who would report matters in the public interest, its provisions should be widely publicised.

Additional efforts could be made to assist those who have reported white-collar crimes in the public interest by establishing a fund to provide compensation for financial loss suffered as a result of their reporting. This could be achieved by setting aside part of the funds obtained through criminal confiscation legislation, if the Commonwealth were agreeable to taking these out of consolidated revenue.

Inducements of this kind are likely to improve the reporting of white-collar crime. The new Act outlined above certainly appears to provide an appropriate framework for the Victorian public sector, but the private sector is likely to need further attention. In one submission to the Committee it was thought that whistleblower protection should be introduced in the Victorian private sector in terms similar to those in the public sector.[46] Helpful initiatives may include guarantees of anonymity where this is necessary to protect a business reputation; assistance in reducing the personal costs and time associated with the investigation and prosecution of a matter, perhaps by streamlining interviewing procedures and reducing the need for senior witnesses to be present in court for lengthy periods; and the use of documentary evidence in preference to oral testimony wherever possible. Appropriate use of awards of costs to assist witnesses should also be considered and scales of witness expenses increased to realistic levels. The use of telephone 'hotlines' may be another way to enable employees to report suspected crimes to management.

In the case of the health care professions, proposals have been considered that would require colleagues to report individuals whom they suspect of having acted illegally. If this idea is to be implemented, then appropriate protection is needed to ensure that those who report colleagues in good faith are not sued or otherwise subjected to recriminations. Examples of such policies are the Department of Defence Whistleblower Scheme which seeks to protect those who report fraud in the public interest (Day 2002), and the Australian Federal Police's Professional Reporting Guidelines (Australian Federal Police 1998b) which set out procedures to support police personnel who report matters they believe to be contrary to the stated core values of the Australian Federal Police.

Already s. 162A of the *Trade Practices Act 1974* (Cth) expressly deals with the question of protection of individuals who provide information or documents to the ACCC or to the Australian Competition Tribunal. Penalties of up to 12

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

months' imprisonment for individuals and fines of up to $10,000 for corporations are specified for those who intimidate individuals who report matters (Bhojani 2002).

Investigation and policing

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. The investigation of white-collar crime and fraud offences therefore requires considerable resources which, in the opinion of some, are not presently provided to police, leading to 'dissatisfaction with police investigations of these sorts of offences'.[47]

In Victoria, the investigation of fraud and dishonesty offences is undertaken either by Criminal Investigation Units, for less complex matters, or by the Major Fraud Group for large-scale, complex crimes. The Major Fraud Group at present has 135 personnel, which includes sworn officers as well as specialist unsworn accounting and legal professionals. It is almost three times the size of the next largest fraud investigation agency in Australia.[48]

Another submission to the Committee argued that the procedures of search for evidence under section 465 of the *Crimes Act 1958* (Vic) 'are cumbersome and inefficient. For example, if the police are setting out to trace funds through several bank accounts, they need to obtain a warrant to search for each new layer of documents'.[49] It was also submitted that a general power to search for relevant documents would be preferable.[50]

Where computers are used in the commission of white-collar crimes, particularly economic crimes, difficulties of investigation are exacerbated because offenders are able to disguise their identities and activities through the use of complex electronic technologies. Anonymous E-mailers and encryption devices can shield offenders from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies. As a result, some crimes may not result in a loss at the time of the act itself, and detection may not occur until some time after a loss has accrued in any case, making the process of investigation even more challenging.

47 Named confidential submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 21 August 2002.

48 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

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

50 Ibid.

Although useful in order to protect confidentiality of legitimate information, the use of encryption makes it difficult, and on occasions impossible, for law enforcement and other official agencies to read the communications in question. This has already occurred in the international investigation conducted into the 'W0nderland' group, as previously discussed, in which those involved in distributing child pornography used heavy encryption to prevent law enforcement officers from obtaining evidence. In business contexts, there is a risk that individuals could encrypt important communications and then refuse to decrypt them unless a fee was paid.

The Committee has also been made aware of the increasing use of steganography used to conceal data. Steganography is the process whereby data are hidden within digital graphic files such as GIF or JPEG files on Web pages. To the casual observer, the information is concealed. It is argued that the use of steganography makes detecting and monitoring criminal activities extremely difficult for police. This is now being used in connection with money laundering, banking and financial records and other illegal business activities. One submission to the Committee argued that law enforcement authorities require additional tools, techniques, equipment and training to respond effectively to such developments.[51]

Other issues that may complicate the investigation of computer-based frauds are the logistics of search and seizure during real time, the sheer volume of material in which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible or accessible only after a massive application of decryption technology. Much time and expense may also be invested in decryption of files that could turn out to be deliberate decoys.

Although computer technologies make some aspects of investigation difficult, in other ways they can assist law enforcement officers. For example, computers are able to handle with ease the substantial quantities of evidence and complex financial records that cases of serious fraud entail, and are also able to record patterns of conduct used in previous cases. These abilities can facilitate the identification of repeat offending by the same individual or by others using the same techniques.

In Australia, a relatively small country, there has been a tendency to create a multiplicity of specialist bodies to investigate and prosecute white-collar crimes of various kinds. This is partly due to the multiple layers of federated governance and has often resulted in law enforcement being fragmented and the effective exchange of intelligence and operational information made difficult. Often the work of bodies is duplicated, or important issues may be left unexamined through agencies believing that another entity has responsibility. This will frequently work to the advantage of offenders, who

51 Submission from P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 15 August 2002.

may be able to delay or avoid detection and prosecution due to a lack of coordination on the part of law enforcement agencies (see Zervos 1992).

An additional problem relates to various organisations, previously controlled centrally by government agencies, but now privately run. The privatisation of utilities and telecommunications carriers, for example, has resulted in law enforcement agencies having to pay substantial fees for information obtained from them.

Some private sector entities, such as Internet service providers, are also unable or unwilling to assist law enforcement agencies with their inquiries where data are not kept, or at least not in a form suitable for investigatory purposes.

To be effective, public and private sector bodies that engage in the investigation of white-collar crime will be required to liaise closely with law enforcement personnel and prosecutors to ensure that evidence is obtained in such a way as not to prejudice its use in criminal trials, and is not lost or damaged. Such cooperation already occurs in many agencies, such as ASIC, which works closely with private insolvency practitioners.

In submissions to the Committee it was stated that certain Criminal Intelligence Units (CIUs) in Victoria have been reluctant to deal with matters involving complex economic crime. This was seen to be due to lack of resources, unsatisfactory sentencing outcomes, and the perception that victims had failed to take preventive measures against the risk of fraud. Often, it was submitted, cases were classified as being insufficiently complex for investigation by the Major Fraud Group, but too complex for ordinary CIUs, resulting in those matters being overlooked. The high workload of the Major Fraud Group also meant that investigations were subject to long delays.[52] Another problem identified relates to the allocation of certain matters between specialised Divisions within Victoria Police (such as the Major Fraud Group, the Organised Crime Squad, the Tactical Response Squad, and the Asian Squad) where an overlap in their jurisdiction occurs.[53]

It may be that consultants trained in policing methods, forensic accounting, or legal procedures need to be employed by both public sector and private sector agencies in order to expedite the investigation of serious fraud. Once a preliminary investigation has been completed, the matter would be referred to the appropriate fraud enforcement and prosecution agencies, which should then be able to deal with it more expeditiously and with less cost to the state.

Recently, initiatives have been taken to establish comprehensive training programs for those involved in the investigation of fraud.[54] Both the Victoria

52 Submissions from A. Bowles, Corporate Crime Liaison Group, and an unnamed confidential respondent, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, August 2002.

53 Anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

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

Police Major Fraud Group and the NSW Police Service's Commercial Crime Agency have fraud investigators' courses conducted by tertiary educational institutions. In Victoria, training is being delivered by the La Trobe University Fraud Investigators' Course, the Corporate Crime Liaison Group, the Financial Institutions Consultative Committee, and the Victoria Police Economic Crime Course.[55] These courses are now becoming open to non-police investigators, which will help to ensure that all 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 coordinated way.

More general investigations have also begun into how policing of fraud offences can be improved. In New South Wales, for example, the Police Minister's Advisory Council has established a Ministerial Taskforce to examine a number of issues to do with the policing of fraud. In particular, the Taskforce will examine avenues for exchange of information between police and other agencies in both the public and private sectors.

Cross-border issues

Additional problems occur in mobilising the law where offenders have fled the jurisdiction or moved assets overseas in order to evade confiscation. In many cases of electronic fraud, suspects will never even have set foot in the victim's country. The advent of digital technologies has also meant that many white-collar crimes now involve a cross-border aspect, with offenders and victims being located in different jurisdictions.[56] This creates a problem in determining where the offence has occurred and therefore which law to apply, as well as a problem in obtaining evidence and ensuring that the offender can be located and tried before a court. These complex legal issues are of jurisdiction and extradition.

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 E-mails, from 1993 to 1999. He was charged with stalking under the existing section 26A 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 vividly highlighted the problem of the extra-territorial application of the offence.

On 10 October 2002, the Crimes (Stalking and Family Violence) Bill 2002 (Vic) received its second reading in the Legislative Assembly. The proposed amendment would cause the offence of stalking (including 'cyberstalking', by

55 Discussed in submissions from A. Bowles, Corporate Crime Liaison Group, and P.R. Hornbuckle, Victoria Police, to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, August 2002.

56 Noted in an anonymous submission to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 12 August 2002.

E-mail 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. Although cyberstalking may bear little resemblance to electronic fraud, the cross-border enforcement challenges are very similar.

It is also important to note that the reform of legislation to create an applicable offence is only the first step toward resolving cross-border problems. Had the facts of the case described above been that an offshore Internet user was 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 cooperative 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 cooperation 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.

The most recent findings of the Internet Fraud Complaint Center, particularly the diverse countries from which fraudsters have been found to operate, highlight the multi-jurisdictional nature of Internet fraud (Internet Fraud Complaint Center 2002). 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 cooperation, including the facilitation by local authorities of foreign proceedings against Australian fraudsters, should be in place if we hope to secure the cooperation 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). In any international law enforcement operation the recovery of the proceeds of crime is a complex question of intermeshing separate, and to a greater or lesser extent incompatible, procedures and chains of authority. Across different legal systems, there is a 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. This is 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 *United Nations Convention Against Transnational Organized Crime*, adopted unanimously by the General Assembly on 15 November 2000 (Resolution 55/25), offers 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 cooperation in expediting the seizure and confiscation of the proceeds of crime.

Prosecution

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.

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 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.

During this Inquiry, a view was expressed to the Committee 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.[57]

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 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 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 educated, professional adults but also self-taught teenagers who commit the online 'white-collar crimes' at issue here. 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

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

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 principal difficulties relate 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, and to the length of time such trials take, which is often exacerbated in cases of criminal conspiracy by having multiple defendants and multiple charges.

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. (Of course, as noted above, it has also has given rise to new offences of unprecedented technicality.)

In addition, legal practitioners are now closely regulated with respect to the length, manner and nature of material that 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. These reforms have not yet been rigorously evaluated, and thus 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).

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.

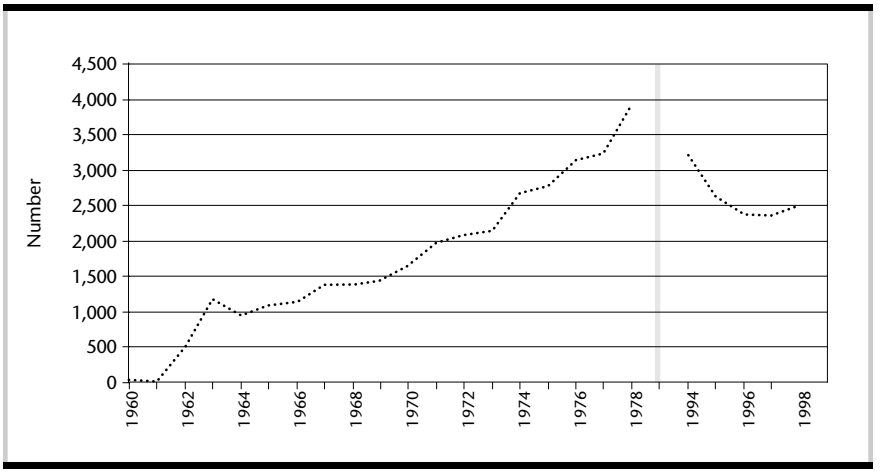
Finally, jurors and lay witnesses in these cases should be provided with information that will enable them to understand the latest court procedures.

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. This, it was submitted, would reduce the length and cost of fraud trials.[58]

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.

For Magistrates' Courts, Figure 6.1 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 6.1: Victorian Magistrates' Courts, principal proven fraud offences, 1960–99

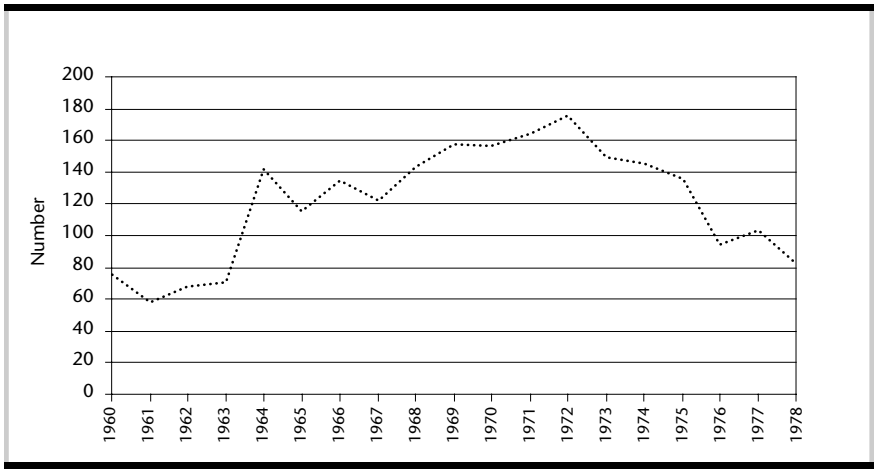


See: Notes to Appendix D for sources, raw data and definitions of offence categories used. Break indicates years for which statistics were unavailable.

For the higher courts (County Court and Supreme Court), Figures 6.2 and 6.3 show the number of sentences given for fraud offences (as variously defined) between 1960 and 1996 – these are shown in two separate figures to take account of the offence classification changes in 1978 which make the figures not directly comparable. Details of the data presented in Figures 6.1 to 6.3 are contained in Appendix D.

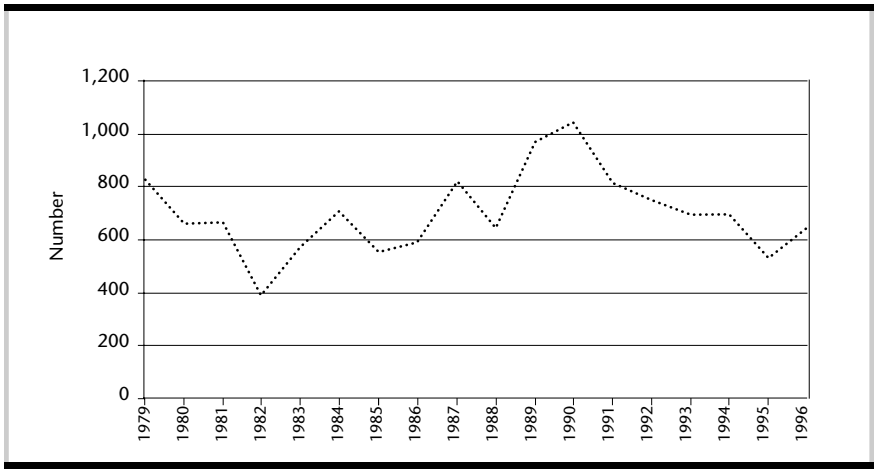
58 Ibid.

Figure 6.2: 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 6.3: Victorian higher courts, principal proven fraud offences, 1979–96



See: Notes to Appendix D for sources, raw data and definitions of categories used.

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).

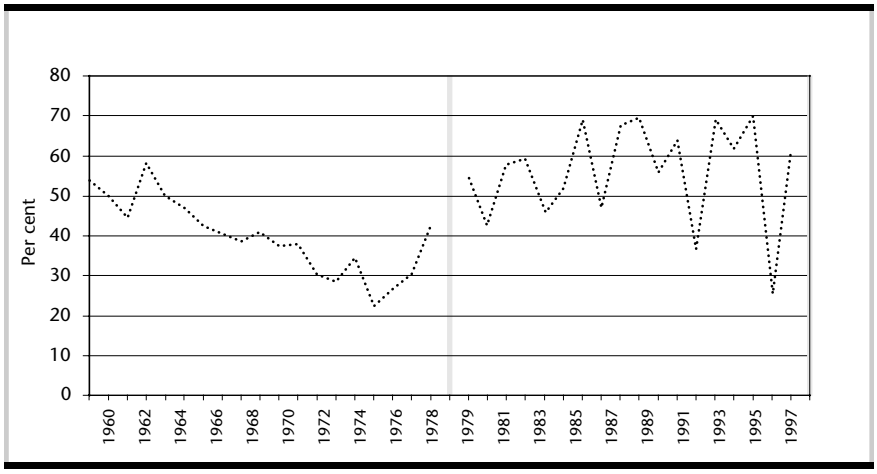
Little research has been carried out in Australia on the manner in which white-collar offenders are dealt with following a criminal trial. In a study of a sample of 50 completed cases handled by the Major Fraud Group of the Victoria Police between January 1990 and October 1994, it was found that 68 per 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.

Details of the sentences given in the higher courts since 1960, and for Magistrates' Courts from 1997 to 1999, are set out in Appendix D.

It has been argued that white-collar offenders tend to receive non-custodial sentences more often than custodial sentences. Reasons given for this include that they are often first-time offenders; have cooperated with the police; have made financial restitution for their offences; may have already 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 previously been persons of high standing in the community.

Statistics related to this question have been calculated from official figures published between 1960 and 1996. Figure 6.4 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. It can be seen that more than half of the sentences given for fraud offences are custodial in nature, and that this proportion has increased gradually since the 1970s, despite the vastly increased range of available sentences such as community based orders.

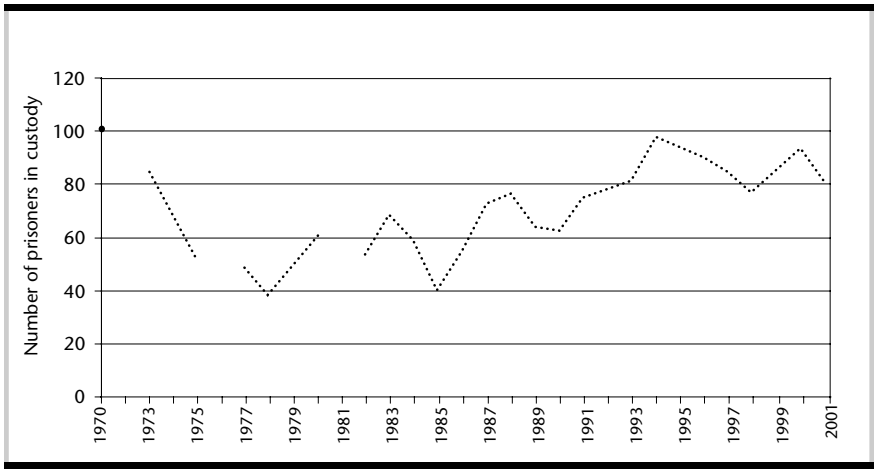
Figure 6.4: Percentage custodial out of total Victorian principal proven fraud offences in higher courts, 1960–97



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, prison stock figures (that is, the number of prisoners in custody whose most serious offence was fraud/deception at 30 June each year) have shown a general increase since the 1970s. The trends are shown in Figure 6.5, the raw data and the relevant category definitions for which are set out in Appendix D.

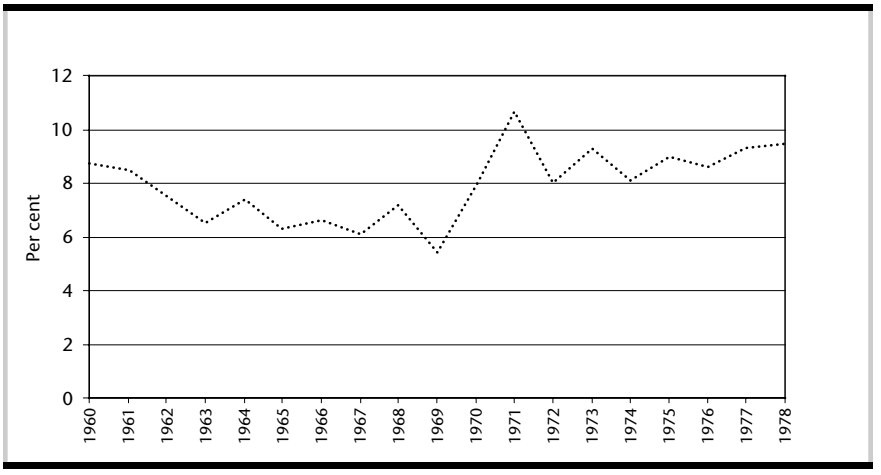
Figure 6.5: Victorian fraud prisoners in custody, 1970–2001



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 six and ten per cent of the total prison population between 1960 and 1979 (see Figure 6.6).

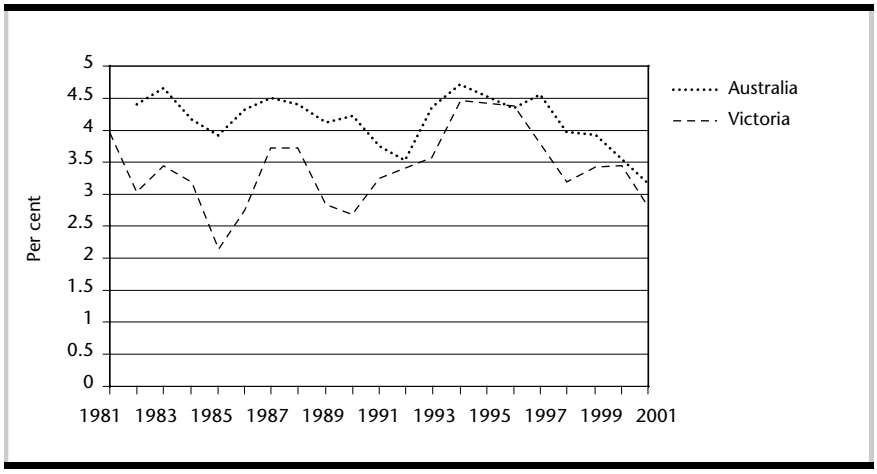
Figure 6.6: Percentage of prisoners' fraud offences out of total prisoners' offences, 1960–78



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 1980 and 2001, Figure 6.7 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 2000–2001, for example, 3.17 per cent of the Australian prison population was imprisoned for the most serious offence of fraud and misappropriation while in Victoria only 2.8 per cent of the Victorian prison population was imprisoned for the most serious offence of fraud and misappropriation. 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 6.7: Percentage fraud offence prisoners out of total prisoners in custody, 1980–2001



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).

On other occasions, sentences of substantial terms of imprisonment have been awarded (see Appendix D for details).

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, p.35). 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. 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).

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. 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 meaning 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 noted the serious consequences suffered by her and her family during the term of the offender's imprisonment. In addition, she noted the absence of effective rehabilitation offered to her husband during the period of his incarceration.[59]

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

59 Submission from G. Calabrese to the Drugs and Crime Prevention Committee, Inquiry into Fraud and Electronic Commerce, 6 July 2002.

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) is beneficial and deserves increased publicity.

Other avenues of redress

Civil action

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.

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.

Professional regulatory action

Victims may lodge a complaint with licensing authorities in cases where fraud is perpetrated by 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 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 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 conducted adversarially and 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. 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 two 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).

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).

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 New South Wales, the Office of the Legal Services Commissioner 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.

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.

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 that govern 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 ASIC, the ACCC, Departments of Fair Trading, Ombudsmen and Complaints Commissioners within certain professions.

As such, dishonest conduct may be scrutinised from a range of perspectives that are both time consuming and expensive to administer. Each system also has conflicting aims and overlapping sanctions.

Questions to consider

Are current dishonesty offences adequate for the prosecution of cases of fraud and deception that occur in Victoria at present?

What new dishonest practices have arisen or may yet arise, that are not covered by existing legislation?

Would the introduction of a general dishonesty offence be an appropriate legal reform in Victoria?

Should Victoria implement the Commonwealth Model Criminal Code provisions that relate to offences of theft, fraud, bribery and related offences in full, or with what alterations?

Should Victoria enact legislation comparable to the United States *Identity Theft and Assumption Deterrence Act* of 1998?

Should a new criminal offence be created proscribing the importation or possession of devices that are to be used for criminal activities (such as the

production of counterfeit credit cards through the use of skimming, and other devices)? If so, how could legitimate use of such technologies be protected?

Should a new criminal offence be created proscribing the possession and or use of counterfeit or altered plastic cards for use in dishonest activities?

How effective has Australian legislation dealing with information privacy been in preventing fraud and to what extent do current information privacy/data protection laws meet our international standards in respect of human rights and trans-border data flows? What changes might be recommended?

Should professionals be under legal obligations to report instances of dishonesty that come to their attention?

In what ways can those who report fraud offences in the public interest be protected against reprisals?

How well do international proceedings for the recovery of stolen monies currently operate when initiated by Victoria and when sought within Victoria?

What reforms are desirable to enhance the extra-territorial operation of electronic fraud-related offences?

In what ways can Victorian laws of search and seizure of evidence be improved to accommodate the difficulties observed at present in cases of complex fraud and electronic crime?

How adequate is the level of funding provided to law enforcement agencies for the investigation of serious and complex fraud in Victoria? What alternative funding arrangements could be provided from both the public and private sectors?

To what extent is the investigation of cases of fraud and white-collar crime duplicated by various Victorian and Commonwealth agencies (including police, consumer complaints authorities and professional regulatory agencies)? How can this be avoided?

Should trial by jury in cases involving complex fraud and electronic crime be replaced with trial by judge alone, or trial by a judge and a panel of specialist assessors?

How should Victorian courts deal with electronic fraud offences committed by minors? Should youth be regarded as a mitigating factor?

What might be done to improve the provision of advice and information about online shopping to members of the public?

What can Victoria do to improve the avenues for making complaints about fraud and unfair business practices?

Should organisations in the private sector be linked directly through an online database to Victoria Police for the purposes of reporting fraud information and intelligence?

7. Key Issues for the Future

Introduction

This Discussion Paper 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 Discussion Paper has primary relevance to Victoria, hopefully the solutions that have been canvassed here may have relevance and will be coordinated with those in other places.

This final chapter summarises some of the key areas discussed as well as the primary directions for future research.

Improving sources of information and statistics

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 the victims of fraud and white-collar crime to be persuaded to report their victimisation so that the matter can be recorded for strategic and statistical purposes and so that action can be taken. 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.

Improving public and business education

There is also a need to enhance knowledge of dishonest criminal activities among potential victims. Law enforcement agencies are well placed to share certain limited kinds of information with private citizens, businesses, and public sector agencies alike, a point stressed by the Corporate Crime Liaison Group in its submission to the Committee[60]. 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, we have seen the development of an Electronic Commerce Code of Conduct, 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 dissemination of basic information on the prevention and control of white-collar criminal activities and the 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, including lists, for example, 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

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

and deceptive practices – the Consumer World web site has over 1,400 links to consumer protection and regulatory agencies (http://www.consumerworld.org).

The Australian Competition and Consumer Commission's web site also gives advice on pyramid selling schemes, business opportunity schemes, and fraudulent prizes and lotteries (ACCC 2001). Examples of recent and prevalent deceptive practices are listed along with the legal penalties which 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 2001). Similar advice is available in Britain at the Office of Fair Trading (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.

Coordinating regulatory efforts

The ease with which fraud transcends domestic and international jurisdictional boundaries, especially in the electronic commerce context, necessitates a high degree of cooperation 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 as widely as possible among law enforcement and regulatory agencies so that appropriate action may be taken as soon as possible.

National approaches such as the new Australian Crime Commission 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 Corporate Crime Liaison Group, which was established by a number of firms of accountants and consultants.[61]

61 Ibid.

In addition, coordination is necessary between Commonwealth and state 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.[62] 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.

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. For example, on 26 June 2002 the South Australian District Court sentenced former chief financial officer of retailer Harris Scarfe, Alan Hodgson, to six

62 ibid.

years' of imprisonment with a non-parole period of three years. He had pleaded guilty to 19 charges of failing to act honestly as a corporation officer, six counts of using his position to gain advantage or cause detriment, and seven counts related to giving false information about the company's financial performance. The judge expressed the need for the sentence to serve as a deterrent (Wood 2002; *Sydney Morning Herald* 2002a).

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 eleventh 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 the case of white-collar offenders who can be said to carry out their activities on the basis of some rational calculation, deterrence remains an important component of crime 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 publicised. If white-collar crime is to be contained, appropriate preventive measures need to be taken in conjunction with well-publicised official action.

Final observations

One of the outstanding lessons that emerges from any sustained examination of the impact upon policy and law wrought by the Internet is that the same structural properties of information networks that underpin the legitimate commercial, educational and socio-cultural opportunities, which many are so keen to grasp, are also ultimately responsible for most of the accompanying risks. As Hardt and Negri note:

> The original design of the Internet was intended to withstand military attack. Since it has no center and almost any portion can operate as an autonomous whole, the network can continue to function even when part of it has been destroyed. The same design element that ensures survival, the decentralization, is also what makes control of the network so difficult. Since no one point in the network is necessary for communication among others, it is difficult for it to regulate or prohibit their communication (2000, p.299).

The online environment is, therefore, a fluid place in which perfect regulation is impossible to achieve. The so-called 'great firewall' of China, instigated by the Chinese government in an attempt to prohibit its Internet users from viewing, amongst other things, politically provocative material, has proved to be less than successful in achieving its objective. The arrest in China on 3 June 2000 of Huang Qi, founder of that country's first human rights web site, saw his supporters quickly copying the site to a server based in the United States, thereby preserving access for Chinese citizens (Neumann 2001). Of course, it is not just political content that finds a way to survive online. Pornography, hate speech, terrorism, organised crime and fraudulent activity of every description also thrive on the Internet.

The challenge for Victoria lies in responding to the risks of fraud, in both the terrestrial and online worlds, in such a way that commerce continues to thrive while risks of fraud are minimised.

Appendices

Appendix A: List of Written Submissions Received

Submission Number	Name of Individual/Organisation	Date Received
1	G. Calabrese	6 July 2002
2	G. Griffiths and M. Griffiths	8 July 2002
3	J.W. Cameron, Auditor-General Victoria	13 August 2002
4	P.S. Clark	15 August 2002
5	N. Jensen, AUSTRAC	15 August 2002
6	P.R. Hornbuckle, Victoria Police	15 August 2002
7	Named confidential submission	21 August 2002
8	A. Bowles, Corporate Crime Liaison Group	30 August 2002
9	Anonymous submission	12 August 2002

Appendix B: List of Oral Submissions Received

Submission Number	Name of Individual/Organisation	Date Received
1	Andrew Tuohy, KPMG	6 & 30 August 2002
2	Russell Smith, Australian Institute of Criminology	30 August 2002

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

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 1993–2001, 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 & Deception Statistics 1960–2001

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**
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
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	4,798,306
Rate/100,000 population	1,077	942		562	597	659	714	761	812	787	620
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
Average Value Stolen $	3,926	2,676		Not Recorded	2,619	3,225	4,904	7,194	31,859	7,555	3,076
Magistrates' Court(8)				**1994**	**1995**	**1996**	**1997**	**1997-98**	**1998-99**	**1999-00**	**2000-01**
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
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**	**1998**	**1999**	**2000**	**2001**
ADU/Bond	133	28	18	8	52	10					
ICO (>92)	-	28	0	0	2	14					
Fine	29	11	4	6	4	4					
Susp	261	144	183	166	319	184					
UCW	89	17	60	25	21	29					
ADTT/ADDP	0	0	1	0	0	1					
CBOM	12	1	0	0	2	1					
Other	0	0	2	0	0	9					
Custodial < 1yr	124	214	129	169	76	231					
Custodial 1-2yrs	104	195	165	170	24	98					
Custodial 2-3yrs	28	74	86	145	23	34					
Custodial 3-4yrs	9	24	21	6	4	25					
Custodial 4-5yrs	24	11	20	3	1	8					
Custodial 5-10yrs	2	1	7	1	1	0					
Custodial 10+yrs	0	0	0	0	1	0					
Sentences for all fraud offences	815	748	696	699	530	648	Not Available	Not Available	Not Available	Not Available	Not Available
% Custodial per total sentences	35.7	69.4	61.5	70.7	24.5	61.1					

cont...

Sentenced Prisoners in Custody(5)	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
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
No of Vic fraud prisoners	75	78	81	98	94	90	85	77	86	94	81
% 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
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
No of Aust fraud prisoners	563	549	691	709	700	690	753	682	723	635	574
% 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

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.

(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 , Courts and Tribunals Services Division, Department of Justice, Melbourne.

1980 to 1996 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. 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 2000-2001 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:

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 2000–2001

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**					
(References are to the Victorian *Crimes Act* 1958 unless otherwise stated)	**Statutory reference**	**< $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.

Offence description	Statutory reference	FINANCIAL YEAR 1999/00 Number of offences recorded per $ value range					
(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.

Appendix F: Number of Miscellaneous Fraud and Electronic Commerce-related Offences Recorded by Police 1993-94 to 2000-2001

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001
Computer-related offences									
Unauth Obstruct lawful use of computer (Other)	Crimes Act 1914 (Cth) s. 76E(b)	-	-	-	-	-	N/A	0	1
Unauth Interfere with computer (Other)(1)	As above	-	-	-	-	-	71	0	3
Enter computer system – no authority (Other)	Summary Offences Act 1966 (Vic) s. 9A	1	6	1	31	13	61	19	6
Gain access to computer – no authority (Other)	As above	1	0	1	1	3	14	5	43
Extortion/blackmail									
Publish/threat publish libel to extort (Other)	Wrongs Act 1958 (Vic) s. 9	0	0	0	0	1	1	0	0
Blackmail (Other)	s. 87	91	129	64	89	114	93	76	93
Extortion-threat to destroy property (Other)	s. 28	1	3	1	8	13	2	3	1
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

cont...

** 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
Unregistered doctor-take/use title (Other)	As above s. 62(1)(a)	-	3	5	0	0	0	0	0
Use title reg medical prac when not reg (Other)	As above	-	0	0	0	0	1	0	0
Practice as psychologist-Not registered (Other)	Psychological Practices Act 1965 (Vic) s. 39(1)	0	0	0	0	0	1	0	0
Advertise as psychologist-not registered (Other)	As above s. 29(1)	0	1	0	0	0	0	0	0
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
LMTC Make false entry in dealings book (Other)	Motor Car Traders Act 1986 (Vic) s. 35(3)	0	0	0	0	0	2	8	0
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
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. 81(1)	N/A	N/A	N/A	2	123	284	170	162
Bring money to Vic – being proceeds of crime (Handle Stolen Goods)	Confiscation Act 1997 (Vic) s. 123(1)	-	-	-	-	-	10	9	2

cont...

Offence Description	Statutory reference**	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998	1998-1999	1999-2000	2000-2001
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
Steal mail from post (Theft (Other))	As above s. 85K(1)(c)	0	6	1	0	1	4	78	3
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
Obtain Drug by False Representation (Drugs (Possess/Use))	As above s. 36B(1)(a)	0	0	0	1	23	1	13	5
Harassment									
Stalk another person (Crimes Act) (Harassment)	s. 21A(1)	-	60	383	695	959	836	709	852
Use phone service-menace/harass/offend (Harassment)	Crimes Act 1914 (Cth) s. 85ZE	598	1461	1710	2537	2350	1157	11	1
Open/tamper with mail (C'wealth) (Harassment)	As above s. 85L(1)	0	4	5	5	9	5	59	2
Cause mail to be wrongly delivered (Harassment)	As above	0	1	0	2	0	0	0	0
Send postal message-forged signature (Other)	As above s.85T(a)	0	1	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
Send postal message-sign fictitious name (Harassment)	As above s. 85T(b)	0	0	1	0	1	0	0	0
Cause phone carrier supply free service (Harassment)	As above s. 85ZF(b)	0	0	0	0	1	0	1	0
Defraud carrier of fee payable telecomm (Harassment)	As above s. 85ZF(a)	0	0	0	0	4	0	1	0
Defraud phone carrier of fee/charge (Harassment)	As above	0	2	0	102	4	0	0	0
Cause phone communication be misdirected (Harassment)	As above s. 85ZD	0	0	0	0	2	0	0	0
Tamper phone facility-hinder operation (Harassment)	As above s. 85ZG	0	0	1	1	42	36	26	5
Knowingly interfere with a facility (Harassment)	As above s. 85ZJ	0	0	0	0	14	177	132	17
Knowingly tamper with a facility (Harassment)	As above	0	0	0	0	0	32	7	1
Recklessly interfere with a facility (Harassment)	As above	0	0	0	0	0	3	3	0
Recklessly tamper with a facility (Harassment)	As above	0	0	0	0	1	7	2	0
Interfere/tamper with phone facility (Harassment)	As above	16	12	1	2	3	0	0	0

Notes to Appendix F

- *Source* Victoria Police *Statistical Review* 1993-2001
- 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.

Bibliography

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/ (visited 14 October 2002).

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 (visited 9 October 2002).

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 (visited 11 September 2002).

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, Sydney.

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 (visited 18 October 2002).

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.acpr.gov.au/publications2.asp?Report_ID=103 (visited 18 October 2002).

Australian Associated Press 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 (visited 11 October 2002).

Australian Associated Press 2002b, 'Man faces court over CityLink credit theft', *NineMSN News*, 8 August. At, http://news.ninemsn.com.au/National/story_36996.asp (visited 11 October 2002).

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 2000c, *Household Use of Information Technology, Australia* (Cat No 8146.0), Australian Bureau of Statistics, Canberra.

Australian Capital Territory 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 1997, *International Internet Sweep Day 1997*. At, http://www.accc.gov.au/ecom2/Inter_net_Sweep_97.htm (visited 17 October 2002).

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, visited 14 October 2002. (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 (visited 17 October 2002).

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 (visited 12 October 2002).

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 (visited 17 October 2002).

Australian Federal Police 1991–2000, *Annual Reports 1991–92, 1992-93, 1993-94, 1994-95, 1996-97, 1998–99, 1999–2000*, Australian Federal Police, Canberra.

Australian Federal Police 1998b, *Professional Reporting Guidelines*, Version 24 June, Australian Federal Police, 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 (visited 20 October 2002).

Australian Securities Commission (ASC) 1996, *Phoenix Companies and Insolvent Trading*, ASC Research Report, Sydney.

Australian Securities and Investments Commission 1993–2000, *Annual Reports 1993-94*, *1994-95*, *1995-96*, *1996-97*, *1997-98*, *1998–99*, *1999–2000*, Australian Securities and Investments Commission, Sydney.

Australian Transaction Reports and Analysis Centre 1999, 'Great tax results', *AUSTRAC Newsletter*, Spring, p.1.

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.

BBC Online 1999, 'How Leeson broke the bank', 22 June. At, http://news.bbc.co.uk/1/hi/business/the_economy/375259.stm (visited 12 October 2002).

BBC Online 2002, 'What surfers are doing on the net', 11 October. At, http://news.bbc.co.uk/2/hi/technology/2310131.stm (visited 17 October 2002).

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. 2000prof, 'Are killer hack attacks coming?', ZDNet, 17 December. At, http://www.zdnet.com/zdnn/stories/news/0,4586,2665640,00.html (visited 8 August 2001).

Bhojani, S. 2002, 'The professions and whistleblower protections', in *Crime in the Professions*, ed. R.G. Smith, Ashgate Aldershot, pp. 139-50.

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.

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/ 35166639324F7B5DCC2568AC0010C1D3!opendocument (visited 14 October 2002).

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.

Cant, S. 2001, 'New digital ID on the way', *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.

Churchill, D. 1997, 'Tricks of the trade', *Police Review*, vol. 105, no. 5435, pp.24–5.

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 (visited 11 October 2002).

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 (visited 11 October 2002).

Commonwealth Attorney-General's Department 2002, *Commonwealth Fraud Control Guidelines*, 13 May 2002. At, http://www.law.gov.au/aghome/commprot/crjd/LECD/guidelinesmay.htm (visited 12 October 2002).

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 (visited 9 October 2002).

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 (visited 14 October 2002).

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 (visited 9 October 2002).

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 (visited 16 September 2002).

Consumer Affairs Victoria 2002, *M-Commerce. What is it?What Will it Mean for Consumers?* Department of Justice, Melbourne.

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 (visited 17 October 2002).

Cook, V. 1999, 'Trust me, I'm a computer', *Communications Newsletter*, September, pp.14–15.

Cox, R. J. & Wallace, D.A. (eds) 2002, *Archives and the Public Good: Accountability and Records in Modern Society*, Quorum Books, Westport Connecticut.

Council of Europe 2001, *Convention on Cybercrime (Status Report)*. At, http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=&DF= (visited 2 October 2002).

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.

Dancer, H. 2000, 'K2 uncovers GST keyhole', *The Bulletin* (Australia), 11 July, p.76.

Day, C. 2002, 'Fraud control in the Australian Defence organisation',in *Crime in the Professions*, ed. R.G. Smith, Ashgate Aldershot, pp.109-14.

De Maria, W. 1995, 'Whistleblowing', *Alternative Law Journal*, vol. 20, no. 6, pp.270–81.

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.

Dearne, K. 2002, 'ISPs lead fraud crackdown', *Australian*, 12 February, p.25.

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) 2002, *Shopping on the Internet: Facts for Consumers*. At, http://www.dcita.gov.au/Article/0,,0_1-2_1-4_13815,00.html (visited 14 October 2002).

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 (visited 14 October 2002).

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 (visited 5 July 2000).

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 (visited 5 July 2000).

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/dab0606eefd3be6bca256ab0003f4687/16c44eb612cd81deca256c1300790fd3/$FILE/DOJWhistleblowersProcedures_Jul02.pdf (visited 26 September 2002).

Department of Public Works and Services, New South Wales 1999, *Electronic Procurement: Taking Up the Challenge*, Sydney.

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/f3acbc234ff76a45ca256c3a0016a4bc/$FILE/EC4P_brochFINAL.pdf (visited 9 October 2002).

Department of Treasury, Consumer Affairs Division, Australia 2000, *Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business*, Commonwealth of Australia, Canberra.

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.

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.

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 (visited 30 September 2002).

Farrant, D. 1999, 'Pre-paid funeral payments misused', *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 (visited 17 January 2001).

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 (visited 10 October 2002).

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%20Criminals.doc (visited 29 May 2002).

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.

Gavan, K. 2001, Balancing commercial realities with the need for fraud prevention: Justifying the cost and demonstrating the return on Investment, paper presented to the IIR Conference 'Applying Risk Management to Implement a Proactive Fraud Prevention Strategy in Financial Services', Sydney, 19 July.

Geis, G. 1991, 'White-collar crime: What is it?', *Current Issues in Criminal Justice*, vol. 3, no. 1, pp.9–24.

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 (visited 4 October 2002).

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, G. 1999, 'The changing face of legal practice and implications for professional indemnity insurance', *Insurance Law Journal*, vol. 11, no. 1, pp.72–90.

Gray, D. 2000, 'HIC Chases $164,000 Over Suspect Scans', *Age*, 13 April, p.6.

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 1997, *Annual Report 1996–97*, Health Insurance Commission, Canberra

Health Insurance Commission 1998, *Annual Report 1997–98*, Health Insurance Commission, Canberra.

Health Insurance Commission 2001a, *Annual Report 2000–01*, Health Insurance Commission, Canberra. Also at, http://www.hic.gov.au/annualreport/ (visited 27 September 2002).

Health Insurance Commission 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)~ (visited 27 September 2002).

Hirschman, A.O. 1970, *Exit, Voice and Loyalty: Responses to Decline in Firms, Organisations and States*, Harvard University Press, Cambridge MA.

Home Office, Britain 2002, *Entitlement Cards Unit Website*. At, http://www.homeoffice.gov.uk/dob/ecu.htm (visited 2 October 2002).

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.

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 Marketing Supervision Network 2002, *IMSN Activities*. At, http://www.imsnricc.org/imsn/activities.htm (visited 17 October 2002).

Internet Fraud Complaint Center 2001a, *Internet Fraud Preventive Measures*. At, http://www1.ifccfbi.gov/strategy/fraudtips.asp (visited 14 October 2002).

Internet Fraud Complaint Center 2001b, *Internet Auction Fraud*, May. At, http://www1.ifccfbi.gov/strategy/AuctionFraudReport.pdf (visited 17 October 2002).

Internet Fraud Complaint Center 2002, *IFCC 2001 Internet Fraud Report*. At, http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (visited 12 October 2002).

Internet Fraud Watch 2002, *2001 Internet Fraud Statistics*. At, http://www.fraud.org/internet/2001stats.htm (visited 14 October 2002).

Internet Industry Association 2001, *Interactive Gambling Industry Code*, December. At, http://www.iia.net.au/gamblingcode.html (visited 4 October 2002).

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.

Keenan, A. 2002, 'Internet stalkers face 10 years jail', *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 (visited 21 October 2002).

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 Australia, Sydney. At, http://www.kpmg.com.au/content/Services/Services/Financial_Advisory_Services/Forensic_Overview/docs/6208%20Fraud%20Survey%202002.pdf (visited 10 October 2002).

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.

Lanham, D., Weinberg, M., Brown, K.E. & Ryan, G.W. 1987, *Criminal Fraud*, Law Book Company, Sydney.

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 (visited 17 October 2002).

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 (visited 12 October 2002).

Legal Practice Board 2001, *Annual Report 2000–2001*, 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 – visited 21 October 2002)

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.

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 (visited 2 October 2002).

McConvill, J. 2001, 'Contemporary comment: Computer trespass in Victoria', *Criminal Law Journal*, vol. 25, pp.220–227.

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.

Markoff, J. 2001, 'Warning from Microsoft on false digital signatures', *New York Times Online*, 23 March.

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.

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 (visited 9 October 2002).

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 (visited 12 October 2002).

National Fraud Information Center 2001, *Internet Fraud* http://www.fraud.org/internet/intset.htm (visited 14 October 2002).

National Fraud Information Center 2001, 'Telemarketing fraud statistics', Washington D.C. At, http://www.fraud.org/telemarketing/lt00stats.htm (visited 12 October 2002).

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 (visited 13 October 2002).

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 (visited 18 October 2002).

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 South Wales Audit Office 1994, *Fraud Control: Developing an Effective Strategy*, Audit Office of NSW, Sydney.

New South Wales Independent Commission Against Corruption 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 Medical Board 1993, *Annual Report for the Period Ended 31 March 1993*, New South Wales Medical Board, Gladesville NSW.

Newlan, D. 2000, 'Detecting and preventing fraud in the energy and natural resources sector', *Energy and Natural Resources Newsletter*, KPMG, Sydney.

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 (visited 14 October 2002).

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 (visited 26 September 2002).

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/26bda3df47c5ae1c4a256b2c001a03b5?OpenDocument (visited 26 September 2002).

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 (visited 14 October 2002).

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*, (52 Session, 1998–99), Government Printer, Melbourne.

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 (visited 13 October 2002).

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 (visited 14 October 2002).

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 (visited 13 October 2002).

Pearson, G. 1996, 'Naked men, food and water: Marketing law and codes of practice', *Current Commercial Law*, vol. 4, no. 1, pp.21–32.

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 (visited 11 October 2002).

Privacy International 2002, *Entitlement Card Proposal FAQ*. At, http://www.privacyinternational.org/issues/idcard/uk/uk-idcard-faq.html (visited 2 October 2002).

Robinson, R. 2002, 'New laws likely to ban net stalking', *Herald Sun*, 21 September. http://heraldsun.news.com.au/common/story_page/0,5478,5138409%255E11869,00.html (visited 30 September 2002).

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.

South Australian Internet Association (SAIA) 2002, *Code of Ethics and Conduct*. See http://www.saia.asn.au.

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 (visited 29 May 2002).

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 Heineman, Boston.

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 (visited 13 October 2002).

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.

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 (visited 2 October 2002).

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 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 (visited 30 September 2002).

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.

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 (visited 9 September 2002).

Sykes, G.M. & Matza, D. 1957, 'Techniques of neutralization: A theory of delinquency', *American Sociological Review*, vol. 22, pp.664–70.

Taylor, N. forthcoming, 'Under-reporting of crime by small retail businesses', in *Trends and Issues in Crime and Criminal Justice*, 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.

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 (visited 20 September 2002).

Tweney, D. 1998, 'Sex scam points out lack of safeguards in online business', 3 August. At, http://www.tweney.com/prophet/980803prophet.htm (visited 14 October 2002).

Tyree, A.L. 1990, *Banking Law in Australia*, Butterworths, Sydney.

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 (visited 30 September 2002).

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 (visited 11 October 2002).

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 (visited 12 October 2002).

Victoria Police 1960–2002, *Statistical Review of Crime 1960–2002*, 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 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 (visited 9 October 2002).

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 (visited 27 September 2002).

Visa International 2001. At, http://www.visa.com (visited 15 August 2001)

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.

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.

Western Australian Internet Association 1997, Code of Conduct, version 1.03, April 30. At, http://www.waia.asn.au/cgi-bin/db.cgi?db=waia&uid=default&sb1=4&so1=descend&view_records=1&Category=—-&keyword=code+of+conduct&nh=5&mh=1 (visited 10 October 2002).

Western Australian Internet Association 2002, *Spam Code of Conduct, version 1.28*, August 27. At, http://www.waia.asn.au/info/spamcode.shtml (visited 10 October 2002).

Weisburd, D., Wheeler, S. & Waring, E. 1991, *Crimes of the Middle Class: White-collar Offenders in the Federal Courts*, Yale University Press, New Haven.

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 (visited 11 October 2002).

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 (visited 3 October 2002).

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.htm, (visited 20 September 2002).

Worldwide Electronic Commerce Fraud Prevention Network 2001a, *Fraud Test*. At, http://www.merchantfraudsquad.com/pages/test.html (visited 14 October 2002).

Worldwide Electronic Commerce Fraud Prevention Network 2001b, *Shop Safely*. At, http://www.merchantfraudsquad.com/pages/shopsafe.html (visited 14 October 2002).

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 (visited 17 October 2002).

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 (visited 17 October 2002).]

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.