AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 62

Fraud: An Overview of Current & Emerging Risks

P.N. Grabosky & Russell G. Smith

Crime is a changing phenomenon. Some activities which in years past were perceived as gravely threatening to the social fabric are now quaintly archaic. Highway robbery is a case in point. Other activities, such as criminal exploitation of on-line commerce, which were inconceivable less than a decade ago, now pose significant risks to Australia's economy and society. Fraud is one general type of crime which, whilst as old as commerce itself, may be expected to take new forms in the 21st century. In some cases, these forms have already begun to emerge. This Trends and Issues outlines a number of social, demographic and economic developments which may be expected to influence the shape of fraud in years to come. One quickly notes that these trends, and the variety of fraud which may be expected to accompany them, are beyond the capacity of law enforcement agencies alone to control. A subsequent Trends and Issues paper will discuss means by which institutions and resources outside the criminal justice system can be harnessed in furtherance of law enforcement.

Adam Graycar
Director

As we near the turn of the century, Australia is in the midst of profound social, economic, and technological change. Many of these broader developments are inevitable, and some, indeed, are highly desirable. They bring with them, however, a number of risks and anxieties. Recent surveys of some of Australia's largest companies have found that fraud is considered to be one of the principal threats to business and far more worrying than any other type of crime (KPMG 1995; Ernst and Young 1996).

Our purpose in canvassing these trends, and the fraud risks which attend them, is to identify areas where fraud prevention efforts can be mobilised in advance, so that Australia may enjoy the maximum benefits of social and economic change, while minimising the downside consequences.

Globalisation

The "Tyranny of Distance" is no more. It has become trite to suggest that the world is shrinking. Australia now exists in a world which is characterised by unprecedented mobility of information, goods and services, people, cultural artefacts, flora and fauna, even viruses— both those of the microbial variety as well as those which infect one's hard drive.

November 1996

ISSN 0817-8542
ISBN 0 642 24025 6

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 06 260 9200
Fax: 06 260 9201
http://www.aic.gov.au

The globalisation of finance, where electronically mediated exchanges occur in nanoseconds, is far removed from the days where deals were sealed with a handshake, and a man's word was his bond. In recent times, the Barings and Sumitomo experiences, whilst occurring well beyond Australia's shores, have had significant domestic repercussions, with adverse effects on financial markets and commodity prices. In brief, the proliferation of anonymous financial transactions is accompanied by a commensurate proliferation of opportunities for betrayal of trust.

Primary production

For nearly two centuries, Australian primary producers have experienced good times and bad at the hands of overseas markets. The influence of global markets would appear greater today than ever before. While the rapidly growing economies of the Asian region present golden opportunities for Australian producers, they also create incentives for fraud. Consider, for example, commercial fishing. While Asian-driven demand has been a boon to the Australian fishing industry, it has produced two unfortunate consequences. Foreign fishers may be attracted to Australian waters, where they fish illegally, unaware, or in disregard of carefully devised local controls, to the disadvantage of the Australian industry. Australian fishers, mindful of the high prices which their product may fetch, may be tempted to exceed their quotas, and fraudulently understate their catch. This could result in overfishing and the collapse of the entire industry, as occurred with the New England fishery in the United States.

Other forms of fraud, some of which have appeared in recent Australian history, can affect overseas markets to the great disadvantage of Australians. The substitution of inferior products can jeopardise an entire export market, as was the case with the meat substitution scandal of the late 1970s. A spate of company collapses a decade later projected an image of Australian entrepreneurs as irresponsible at best, and of Australian financial markets as unsuitable places to invest. Billions of dollars of export revenue and overseas investment in Australia can be lost when global markets punish what is perceived to be Australia-wide fraud. Given the relatively small size and fragility of its economy by global standards, Australia is especially vulnerable.

Industrial espionage

The globalisation of the economy and the importance of Australia remaining a competitive player require that Australian enterprise take every advantage of overseas business opportunities. Australian companies doing business abroad (and indeed, Australian domestic enterprise as well) should be mindful that the world of international business is in some respects a jungle. Overseas competitors, and nations which might be hosts to Australian investment, may have a strong interest in Australian trade secrets and other economic intelligence. The lengths to which foreign interests might go in order to acquire such information may not adequately be governed by the laws of Australia or, indeed, any other jurisdiction. Industrial espionage by governments and private sector institutions is a fact of contemporary commercial life and recent developments in the technology of intercepting communications make such activities easier to undertake and more difficult to detect than in the past.

Technology

Globalisation is fostered by technology, which in turn facilitates so many other aspects of contemporary life. Dramatic changes in the capacity and accessibility of new technologies have changed the way we are born, the way we live, and the way we die. The breathtaking pace of technological change, perhaps most evident in the convergence of computers and communications, has taken us to the dawn of a new age. In the realm of fraud, expanding "computer literacy" will increase the number of prospective offenders, while new technologies allows easier and cheaper access to a much larger pool of prospective victims.

Electronic funds transfers

The move to a cashless society has significant implications for both law enforcement and society. The advent of so-called "smart cards" which have the ability to store and in some cases to process data, will inevitably invite attempts at electronic counterfeiting. The volume and velocity of financial transfers also pose significant challenges for the interdiction of money laundering and tax evasion (Wahlert 1996), while the advent of cashless payment systems may strike at the root of existing prudential supervision of financial institutions.

The proliferation of electronic funds transfer systems has enhanced the risk that such transactions will be intercepted and funds diverted. Existing systems such as ATMs, and EFTPOS technologies have already been the targets of fraudulent activity, while home banking and Internet shopping with the use of electronic cash will provide rich new avenues of fraud in the future. Most of the large scale electronic funds transfer frauds which have been committed have involved the interception or

alteration of electronic data messages transmitted from bank computers, sometimes with the complicity of bank employees.

Telecommunications

Advances in telecommunications are accompanied by unprecedented opportunities for the theft of telecommunications services (Smith 1996). Internationally, losses sustained through theft of telephone services have been substantial. While the Australian figure is not yet known, telephone fraud in the United States is estimated to amount to the equivalent of A$5.3 billion annually. The ubiquitous cellular telephone has also provided inestimable opportunities for fraud which is said to cost the industry in the United States one million dollars a day.

Demography

Fraud against the elderly

The demographic structure of Australian society is changing quite significantly. Under current projections, the "greying" of Australia, an undeniable demographic trend, will continue well into the 21st century. A significant proportion of present and future retirees possess at least modest assets. As the baby boomers who followed the end of World War Two near retirement age, the growing cohort of senior Australians will possess unprecedented amounts of disposable income. Traditions of trust and openness, historically part of the Australian character, have recently been confronted by an ethos of greed. The darkest side of the entrepreneurial spirit is reflected in those who would exploit the powerless and the vulnerable for personal gain. One may thus predict an increasing risk of fraud against elderly Australians.

This may entail a range of common investment and sales-related frauds, as well as forms of fraud which have traditionally been directed at seniors, such as retirement investment fraud, automobile and home repair frauds.

The ageing of Australian society will also be accompanied by increasing consumption of health services. Regardless of the means by which health services will be delivered or financed, the growth of this industry will provide opportunities for unscrupulous providers. The costs of fraud, waste and various abuses such as over-servicing have reached astronomical proportions in the United States. Australia's current system of health care delivery creates an environment in which similar fraudulent activity is likely, and indeed is already taking place. While some of the American experience may reflect perverse incentives which are unique to the US health system, the ageing of the Australian population will have implications for fraud control.

Australia's ageing population may also become the perpetrators of fraud. Wherever government-funded health and social security schemes have been established throughout the globe, these have been abused by individuals who feel, sometimes with justification, that their needs are not being adequately met and that their lifetime of taxation contributions is not being reflected in the range and standard of services which governments provide. Similar justifications exist in the case of insurance fraud, another area of concern for the future.

It has been suggested that the ageing, less mobile population will be more likely to engage in crimes of fraud than in traditional property offences which require speed and agility for their commission (Albanese 1988). Computer fraud may, for example, be carried out just as easily by the immobile or housebound as by those without such constraints.

Australia's move to a multicultural society, and the corresponding growth of ethnic minorities, may be accompanied by significant numbers of people who may be both linguistically disadvantaged and unfamiliar with basic principles of Australian commerce and finance. As such, they are at greater risk of victimisation at the hands of fraudsters generally. The least fortunate of these may even be vulnerable to exploitation from within their own ethnic group, particularly when assistance is needed in moving funds between countries.

Migration fraud

Since the waning of the convict era, Australia has been an attractive destination for people from around the world. Australia's prosperity and the opportunities which it presents are the envy of many. This will no doubt be enhanced by the increasing attention which Australia will receive in the global media in the years leading up to the Sydney Olympics. The attractiveness of Australia is even greater for individuals from those various places around the world which are afflicted by wars, civil unrest, natural disasters and economic deprivation. One may thus expect continued efforts to enter and remain in Australia illegally. One may also expect persistent, and increasingly sophisticated attempts to fabricate travel documents, and to try other contrivances such as arranged marriages and fraudulent (as distinct from legitimate) claims of political persecution.

Disadvantaged minorities

Despite its status as the "Lucky Country", Australia itself is not without its disadvantaged groups. To the extent that Australia's disadvantaged minorities gain self

determination and financial autonomy, opportunities for abuse of the resources which they control will arise. This is not to suggest that members of a given group are any more or less venal than the general population. Rather, we suggest that crime, and in this case, fraud, follows opportunity. Moreover, diminishing disadvantage is a double-edged sword. Not only does emerging financial autonomy create opportunities for the less honest of those representatives of disadvantaged minorities who may be entrusted with public or private funds, but the disadvantaged individual who commands some disposable income may be particularly at risk of victimisation.

Commerce

Australia is at present experiencing economic change at a dramatic pace. One of the most prominent examples of such change is the growth of the superannuation industry. Over 100 000 superannuation funds currently exist in Australia. In a few short years, vast sums have accumulated, and some estimates suggest that the superannuation savings pool may rise to some A$2000 billion by the year 2020 (Freiberg 1996).

This is not to suggest that persons charged with the stewardship of such funds have unusual criminal propensities, but again, the sheer volume of money constitutes what may be an irresistible temptation to the unscrupulous. Abuses of superannuation funds in the United States and the United Kingdom illustrate the attractiveness of such enormous amounts of money to those who would commit fraud. Short of the risk of outright fraud, the risk of imprudent management cannot be ignored.

Telemarketing fraud

The media of commerce are also changing. The days of face-to-face exchange are yielding to increased sales by means of mail-order and telemarketing. In 1995, telemarketing comprised 25 per cent of the volume of the A$4.5 billion Australian direct marketing industry. While these new media offer greater opportunity and choice for consumers, they also pose greater risk. The amount of telemarketing fraud in the United States has been estimated at between US$15 and US$40 billion dollars per year. The specific goods and services which can be the subject of telemarketing fraud are as varied as the human imagination, and range from phoney contests and lotteries, bogus charitable solicitations, to an infinite variety of products and investments.

The next generation medium will be Internet commerce. By the year 2001, it has been estimated that the value of Internet commerce will range from between A$6 billion and A$600 billion, the actual size depending upon the extent to which secure and accessible payment systems operate. Once again, alongside its attractiveness and advantages as a medium of commerce are the risks which it poses. Authorities overseas have begun to identify a range of "Internet scams" including "work-at-home" businesses, services purporting to improve one's credit rating, and investments in such exotic products as coconut plantations. Developments in telecommunications have begun to provide the basis for, as well as the medium of, telemarketing fraud. High-pressure promotion of paging licenses and pay-per-call investment schemes began to proliferate in the United States during 1995.

Although many fraudulent pitches are quite direct, the Internet provides a vehicle for more insidious marketing. "Disguised advertising" on the Internet is difficult to recognise because it is not always apparent that a product is being advertised. Bulletin boards and chat forums may contain comments or statements about the quality or the performance of products or services. These may in fact be advertisements.

It bears noting that not only are such overseas scams easily accessible in Australia via the Internet, few remedies are available to the unfortunate Australian who might fall victim to such a fraud. Even if one is able to mobilise the law, the chances of locating the fraudster, obtaining extradition, mounting a prosecution, or recovering compensation may be impossible.

Changes which the Australian economy is currently experiencing are accompanied by pain as well as by benefit. Both are accompanied by risk. Those who regard themselves as the victims of microeconomic reform may well seek to extract revenge upon their former employers or upon "the system" generally. This could be manifest in behaviours as diverse as pre-separation embezzlement, or some form of post-separation retaliation involving fraud. Disgruntled former employees with expertise in information technology are in a position to inflict significant damage. In the years to come, when telecommunications and information technology organisations expand and contract in size, the number of displaced individuals with the skills necessary to engage in cyber-warfare may lead to the creation of a significant threat.

Business opportunity fraud

The downsizing of organisations in both the public and the private sectors has begun to generate growing numbers of individuals in mid-career with significant lump-sum payouts. Consequently, there

has been a significant increase in the role and importance of fiduciaries in society, namely individuals such as solicitors, accountants and financial advisers, charged with looking after their clients' best interests, particularly where money is concerned. Already such individuals have been involved in stealing many millions of dollars of their clients' funds which have been provided in good faith for investment or other purposes. With increasing sums of money to invest, the temptations of fiduciary fraud are bound to increase.

In addition to entrusting their funds to financial managers, those with money to invest are within reach of the Australian dream of starting a small business. Unfortunately, they are also within reach of fraudsters who would exploit them. Business opportunity fraud or other "get rich quick" scams may be an unfortunate by-product of Australia's move to a more competitive economy.

One of the easiest avenues into small business is through purchase of a franchise. It has been estimated that in the United States, by the year 2000 over half of all retail sales will occur through franchised establishments; franchising is also a predominant feature of the Australian commercial landscape. Short of the most blatant form of franchise-related fraud, simply taking the new franchisee's up-front money and disappearing with it, there remains the potential for a variety of lesser misrepresentations, such as overstatement of earnings potential and understatement of risks or other hidden costs of a franchise agreement.

Organisations which provide funds to others are also vulnerable to modern forms of fraud. A large industry now exists in establishing false identities and fraudulent credit ratings for people who wish to borrow money but who may be disinclined to repay it. Even organised deception in valuing property which forms the security for loans has been employed by individuals who wish to obtain funds illegally.

Copyright fraud

Patents, trademarks, and designs are all vulnerable to piracy, particularly in the current technological environment which facilitates near perfect counterfeiting and copying. The attractiveness of designer labels to consumers around the globe has inspired blatant imitation in some quarters. Illicit copying of software, videos and compact discs is a growth industry in some countries. In the United States in 1995, there were an average of thirty-one intellectual property loss incidents reported per month resulting in losses of more than US$5 billion (Anonymous 1996). Already, Australia has the unenviable reputation of having the highest incidence of software piracy in the developed world, the costs to the industry of which the Business Software Association estimates to be A$260 million a year (Neiger 1996).

One may also expect that the forthcoming Sydney Olympics may see illicit attempts to exploit Olympic trademarks. Indeed, the Olympic Games, like any occasion at which substantial numbers of people congregate, will have enormous potential for fraudsters intent on exploiting holiday-makers throughout their journey and visit. In particular, the use of credit facilities and plastic transaction cards will permit many fraudsters illegally to obtain money brought to Australia by Olympic tourists. The potential for fraud also exists in the provision of travel, accommodation and sponsorship arrangements associated with the Games.

Public Administration

The very nature of governance in Australia is changing. The public sector is shrinking in size; many functions previously performed by public servants are now being "outsourced", "contracted out" or otherwise devolved upon non-governmental institutions. This may lead to more efficient government, but it is by no means free of risk.

To the extent that this downsizing is experienced by regulatory institutions, their capacity for scrutiny and surveillance may be reduced. If, for whatever reason, the proper functioning of informed markets do not compensate for these regulatory deficits, there may be greater opportunities for exploitation by the unscrupulous. The numerous corporate collapses of a decade ago have been attributed in part to inadequate regulatory oversight (Sykes 1994).

To the extent that regulatory functions are performed by non-governmental institutions, the transparency and accountability of the regulatory process may suffer. At times, there may be tension between commitment to the public good, and a private contractor's private interest. Australia may not be destined to relive some of the more unsavoury experiences from elsewhere, but it is important to acknowledge the risk that some self-regulatory regimes, particularly those based on self-monitoring and reporting, have suffered from fraudulent disclosure (or non-disclosure). To the extent that testing and evaluation services are performed by private institutions, they may be vulnerable to fabrication or negligent performance. One may recall how audit failures, whether they arose from complicity, negligence, or bad luck, underlay many of the corporate collapses

which characterised what we have since come to describe as "the excesses of the 1980s" (*see* Kapardis & Kapardis 1995).

Fraud by government contractors

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

Conclusion

Given the uncertainties and rapid changes which Australia is currently experiencing, it is understandable that some would wish to "turn back the clock". Regardless of whether or not one regards this as desirable, it is no longer feasible. Rather than yearn for the halcyon days of the past, it is incumbent upon policy makers to design policies which maximise the positive aspects of trends which lie before us, and to anticipate and minimise the risks which accompany them. This will involve research activity which examines globalisation, demography, technology, commerce and public administration, and their intersection with fraud and criminal opportunity.

Proactive planning for fraud prevention requires ongoing assessment of risks and the design of appropriate countermeasures to meet them. In predicting the likely course which fraud will follow in the future, it is important to base predictions upon a comprehensive understanding of currently identifiable areas of risk. Being forewarned is, perhaps, the best preventive strategy to adopt. This requires the compilation and analysis of data from a wide variety of governmental and non-governmental sources concerning the manner which current frauds have been perpetrated in order to assess likely vulnerabilities of the future. Only then will it be possible to adopt appropriate risk reduction activities.

References

Albanese, J. S. 1988, "Tomorrow's thieves", *The Futurist*, vol. 22, no. 5, pp. 25-8.

Anonymous 1996, "Espionage: A growing problem", *CJ The Americas*, vol. 8, no. 6, p. 14.

Ernst and Young 1996, "Fraud: The unmanaged risk", Ernst and Young, Sydney.

Freiberg, Arie 1996, *Superannuation Crime*, Trends and Issues in Crime and Criminal Justice No. 56, Australian Institute of Criminology, Canberra.

Kapardis, M. & Kapardis, A. 1995, "Co-regulation of fraud detection and reporting by auditors in Australia: Criminology's lessons for non-compliance", *Australian and New Zealand Journal of Criminology*, vol. 28, pp. 193-212.

KPMG 1995, *1995 Fraud Survey*, KPMG, Sydney.

Neiger, D. 1996, "Software theft can occur in many ways", *Engineers Australia*, May, pp. 22-3.

Smith, Russell G. 1996, *Stealing Telecommunications Services*, Trends and Issues in Crime and Criminal Justice, No. 54, Australian Institute of Criminology. Canberra.

Sykes, Trevor 1994 , *The Bold Riders: Behind Australia's Corporate Collapses*, Allen and Unwin, Sydney.

Wahlert, Glenn 1996, "Implications of the move to a cashless society: Law enforcement" in *Money Laundering*, Research and Public Policy Series No. 2, eds Adam Graycar & Peter N. Grabosky, Australian Institute of Criminology. Canberra, pp 22-8.

Dr Peter Grabosky is Director of Research and Dr Russell G. Smith is a Senior Research Officer with the Australian Institute of Criminology

Submissions for consideration for the Trends and Issues series should be forwarded to:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia