9

The prevention and control of economic crime

Peter Grabosky

Economic crime, by which I refer generally to fraud in its various manifestations, is among the most costly of all criminal activities. Although it would be interesting to determine its cost with some precision, the total impact is unquantifiable. There are a number of reasons why attempts to estimate the costs of economic crime are bound to be futile. First, the most skilfully perpetrated offences are not even detected by victims. Even when an offence is detected, and the victim knows that he or she has sustained a loss, they may be reluctant to report. In the case of an individual, he or she may simply be too embarrassed, and the expectation of recovering lost assets may be remote or nonexistent. In the case of an organisation, they may be concerned about possible damage to their commercial reputation, and decide as a matter of business judgment not to disclose their vulnerability.

Statistics aside, the reasons for being concerned about economic crime should be obvious to many. The essence of fraud is a breach of trust. Trust is the very foundation of commerce and of civil society. Economic crime thus jeopardises basic interpersonal relations, economic development, and in some cases, even the stability of governments. One wonders, for example, what the economy of the former Zaire might have become had its corrupt leadership not plundered the nation's wealth. The collapse of the Albanian regime following massive losses sustained by thousands of citizens in an investment fraud constitutes another example. One could compile a long list of cases, but the purpose of this chapter is to discuss the risks of economic crime and the countermeasures which might be put in place to minimise them. This chapter places special emphasis on computer-related crime, because the convergence of computers and communications will become the dominant factor in commerce in the new millennium.

Crime is a changing phenomenon. Some activities, such as criminal exploitation of online commerce, which were inconceivable less than a decade ago, now pose significant risks to the economy and society of many nations.

Fraud is one general type of crime which, whilst as old as commerce itself, may be expected to take new forms as the twenty-first century progresses. In some cases, these forms have already begun to emerge. This chapter outlines a number of social, demographic and economic developments which may be expected to influence the shape of economic crime in years to come. It is of note that these trends, and the variety of economic crimes which may be expected to accompany them, are beyond the capacity of law enforcement agencies alone to control.

The environment of economic crime

It has become trite to suggest that the world is shrinking. The world is now characterised by unprecedented mobility of information, finance, 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.

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 have had significant global 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.

Varieties of economic crime

There are several major forms of economic crime which confront society in the new millenium. The following categories are not mutually exclusive, but are intended to illustrate the range and variety of economic crime.

Insurance fraud

Insurance is a most important institution, enabling us to spread risk and thereby engage in activities of tremendous commercial or individual benefit. With insurance, however, comes the opportunity for fraud. The fabrication of false insurance claims is as old as the institution of insurance itself. Whether at the hands of opportunistic individuals or criminal organisations, the cost of insurance fraud is substantial and often borne by honest and law-abiding policyholders.

Fraud against governments

Governments are at great risk of fraud. They dispense benefits, and many citizens are not beyond obtaining these benefits fraudulently. They buy goods and services, and many purveyors of these goods and services are not beyond providing inferior products or otherwise inflating their invoices. Governments

raise taxes, and many taxpayers evade payment. Government employees may divert public assets for private use. When governments are defrauded, all honest citizens pay the price. To the extent that funds defrauded would otherwise be spent on worthwhile government programs, the public suffers twice.

Fraud against employers

Organisations, whether in the public or private sector, may be at risk from their employees. Embezzlement or theft of money, goods or services by employees can mean the difference between economic survival and bankruptcy. When an employer's business fails because of employee theft, law-abiding employees are among those who pay the price.

Fraud against consumers

Purveyors of goods and services can cheat their customers in many ways. They may provide defective or inferior products or fail to deliver goods and services altogether. They may advertise their products in a deceptive manner. In the extreme, this can lead to death or injury in the case of dangerous products purported to be safe. At the very least, the consumer or will pay more for a product than he or she should.

Telemarketing fraud

The media of commerce are also changing. The days of face-to-face exchange are giving way to an increased volume of sales by mail-order and telemarketing. Telemarketing may involve the use of the telephone or increasingly the internet, which may well become the dominant medium of commerce this century. While these new forms of media offer greater opportunity and choice for consumers, they also pose greater risk. *Ceteris paribus*, the greater the uptake of new technologies for commercial application, the greater the risk that they will be exploited for criminal purposes.

Fraud against shareholders and investors

The directors of large companies may divert company assets for personal use. When this occurs on a scale sufficient to affect the company's financial performance, shareholders and investors suffer. At the extreme, companies may collapse, leaving investors and creditors at a loss. Endemic fraud can taint an entire economy, leading to capital flight and discouraging foreign investment.

Superannuation fraud

The world's industrialised nations are at present experiencing certain economic changes at a dramatic pace. One of the most dramatic examples is the growth of the superannuation industry, which establishes and manages private pension

funds. Over 100,000 superannuation funds currently exist in Australia alone. Around the world, vast sums have accumulated, and the superannuation savings pool contains trillions of dollars.

This is not to suggest that persons charged with the stewardship of such funds have unusual criminal propensities, but 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.

Bribery and corruption

Public officials may demand or accept a financial or other consideration as a price of doing business. This can erode the legitimacy of an entire government. Companies in the private sector may require side payments from suppliers. In the long run, the cost is borne by consumers. Widespread, entrenched corruption can detract from a nation's economic competitiveness and may discourage foreign investment.

Money laundering

The term is used to describe the process by which the proceeds of crime ('dirty money') undergo a series of transactions which disguise their illicit origins and make them appear to have come from a legitimate source ('clean money'). This makes criminal activity more difficult to detect, can lead to the criminal infiltration of legitimate business, and can distort the economies of small nations.

Telecommunications fraud

As telecommunications services become more widely accessible, the theft of such services becomes more common. From the 'cloning' of cellular telephones, to the unauthorised access and use of telephone switchboards, and the fabrication of stored-value telephone cards, millions of dollars of telecommunications services are misappropriated.

Credit card fraud

There are four basic vulnerabilities of plastic card payment systems.

- Vulnerability of cards to alteration and counterfeiting.
- Vulnerabilities arising from the issue of cards.
- Vulnerabilities arising from card holder identification systems (PINs).
- Vulnerabilities arising from the misuse of cards.

As plastic cards eclipse currency as a method of payment, opportunities for their misuse will increase. The costs will be borne by merchants and by card issuers.

Industrial espionage

The world of international business is in some respects a jungle. Competitors at home and abroad, and nations which might be hosts to a company's investment, may have a strong interest in a company's trade secrets and other economic intelligence. The lengths to which some will go in order to acquire such information are substantial, and at times illegal. Industrial espionage by governments and private sector institutions is a fact of contemporary commercial life. Companies', indeed, nations' competitive advantage may be at stake.

Theft of intellectual property

Copyright infringement can occur quickly and easily, greatly facilitated by the advent of digital technology. Text, video, sound, designer labels and computer software can be copied and reproduced as never before. Unrestrained, such modern forms of piracy can discourage invention and innovation and deprive artists and creators of the royalties to which they are entitled.

Forgery

Currency, negotiable instruments and a variety of other valuable documents may be forged or counterfeited. The advent of digital technology, including scanning and copying, enables almost perfect reproduction. Not only may the recipient be left holding a worthless piece of paper, but forged documents can be used to facilitate a variety of other economic crimes.

Business opportunity fraud

In the industrialised world, the downsizing of organisations in both the public and the private sectors has generated growing numbers of individuals in mid-career with significant disposable income. 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 may wish to start a small business. Unfortunately, they are also within reach of others who can exploit them. Business opportunity fraud or other 'get rich quick' scams may be an unfortunate by-product of nation's transition 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, over half of all retail sales were through franchised establishments in 2000. 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.

Electronic funds transfer fraud

The move to a cashless society has significant implications for both law enforcement and society. Although reducing the use of cash in the community may help minimise traditional forms of bank robbery and theft, new cashless payment systems will create new problems. The proliferation of electronic funds transfer systems will enhance the risk that such transactions may be intercepted and diverted. Existing systems such as automatic teller machines (ATMs), and electronic funds transfer at point of sale (EFTPOS) technologies have already been the targets of fraudulent activity. Most of the large-scale electronic funds transfer frauds that have been committed have involved the interception or alteration of electronic data messages transmitted from bank computers, sometimes with the complicity of bank employees. The development of electronic commerce will be impeded to the extent that the security of electronic transactions is threatened.

Commonalities

One common thread running through most if not all of the types of economic crime listed above is that they are greatly facilitated by recent developments in information technology. This does not mean that we should 'pull the plug' on our computers. Indeed, if mankind were to reject all technologies because of their potential for abuse, we would have rejected the wheel. Rather, we must learn to exploit the benefits of new technologies and manage the risks which accompany them. But we should not underestimate the challenges the digital age poses to those involved in the prevention and control of economic crime.

Where computers are used in the commission of fraud, difficulties of investigation are exacerbated as offenders are able to disguise their identities and activities through the use of complex electronic technologies. Those who seek to mask their identity through the use of computer networks are often able to do so by means of looping or weaving through multiple sites in a variety of nations. Electronic impersonation—colloquially termed 'spoofing'—can be used in furtherance of a variety of criminal activities, including fraud. Anonymous re-mailers and encryption devices can shield one 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 detection or loss until some time after the event, thus making the process of investigation even more challenging.

Other issues which may complicate the investigation of computer-based fraud entail the logistics of search and seizure during real time, the sheer volume of material within 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.

Economic crime in a shrinking world

It is worth noting that not only can many fraudulent initiatives originate on the other side of the globe, but few remedies are available to the unfortunate individual who might fall victim to transnational economic crime. Even if one is able to mobilise the law, the chances of locating the offender, obtaining extradition, mounting a prosecution, or recovering compensation may be minute.

Particular problems arise when financial crimes are committed against a local company or government agency by a person situated in a foreign country. Enlisting law enforcement assistance in the foreign country may be difficult, as their resources are limited and their priorities may well lie elsewhere.

Even where a perpetrator has been identified, two problems arise in relation to the prosecution of offences which have an international aspect. First, the determination of where the offence occurred in order to decide which law to apply; and second, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition.

Additional problems are reflected in the difficulty of exercising national sovereignty over capital and information flows. Jurisdictional issues may arise from transborder online transmission. If an online financial newsletter originating in Albania contains fraudulent speculation about the prospects of a company whose shares are traded on the Tokyo Stock Exchange, where has the offence occurred?

Even if the host law enforcement agencies are willing and able to assist, collection of evidence in the foreign country may be problematic. Distance will be more of an impediment to the thief-taker than to the thief. The cost of sending law enforcement officers abroad to assist in an investigation, or the cost of bringing witnesses from abroad to testify in proceedings, may be prohibitive. Even then, there are often legal impediments which must be overcome. The laws of evidence of one's own country are not likely to be instantly hospitable to all evidence obtained from abroad. In nations where a degree of thought has been given to these issues, mutual assistance arrangements may be reached with selected nations for the collection of evidence on their soil, and special legislation may be enacted to provide for the admissibility in one's own courts of evidence taken abroad.

It must be emphasised that none of these impediments to the investigation and prosecution of transnational economic crime are unique to high technology offences. They exist for more conventional forms of criminality as well. However, their significance is heightened, given the increased opportunities for transnational offences which new technology provides.

Extraterritorial law enforcement costs are also often prohibitive. Moreover, the cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities across nations which, despite prevailing trends towards globalisation, exists only infrequently. This may be less of a problem with fraud than with matters relating to political or artistic expression.

Countermeasures

The extreme diversity of economic crime means that no single institution of prevention or control will suffice. The police alone are unable to cope with economic crime; there can be no 'magic bullet' or panacea. Rather, each separate type of economic crime is best addressed by a combination of countermeasures. Some of these will be governmental, some will lie in the hands of the prospective victim, and some will be at the disposal of third parties.

- The first line of defence against economic crime is awareness of one's vulnerability.

The popular term for this is 'risk assessment'. This applies to the individual consumer or investor, who should become familiar with the basic pitfalls of the marketplace; to companies, who should be aware of the procedures and processes which are likely targets; and to governments, whose various functions (such as payment of benefits and the purchase of goods and services) may be targeted for criminal exploitation.

- The next step is to take necessary precautions.

The key to fraud prevention on the part of organisations, whether public or private, is the development and refinement of a fraud control system. Having identified points of vulnerability, individual systems and processes should be put in place to protect these vulnerabilities from 'attack'. These principles apply to the control of 'electronic' economic crime, those offences committed with or against telecommunications and information systems, as well as the more conventional forms of crime. The foundation for such a system is a management philosophy which is sensitive to fraud risk. The basic elements of such a system are careful recruitment of staff, a culture of integrity and loss prevention within the organisation, and formal procedures for the protection of assets.

The design of systems can be an important means of fraud prevention. The introduction of a requirement that the recipients of public funds have an account

with a financial institution in which the funds can be deposited automatically, has dramatically reduced the risk of lost or stolen cheques and fraudulent claims. Fraud control systems may include technologies as diverse as the requirement that company cheques be signed by two people, to sophisticated systems of biometric authentication (based on physical characteristics such as fingerprints or retinal images) required for access to a computer system.

There are some basic principles for the prevention and control of economic crime.

Audit

The scrutiny of a company's accounts by an independent auditor is an important safeguard against economic crime. It is by no means fail-safe, as accountants often fail to detect irregularities, but the very necessity of having to prepare accounts in a form suitable for independent scrutiny and then subjecting them to a degree of examination is an important first step.

Transparency

It was once said that 'sunlight is the best disinfectant'. Procedures for the public disclosure of basic aspects of a government's or a company's operations can help safeguard against a variety of crimes. Freedom of information legislation can facilitate citizen access to government information. This is not to suggest that trade secrets—or military secrets for that matter—be made available to anyone who wants them. Rather, it means that fundamental information is available to keep markets and citizens informed.

The requirement that organisations in both the public and private sectors publish regular accounts which disclose details of income and expenditures, including the salaries of executives and liabilities relating to environmental pollution, has become an international standard of best practice. Markets are beginning to expect nothing less.

Procedures for independent review of administrative decisions

The possibility of bias or other irregularities in the administrative decisions of governments can be addressed through the system of administrative law (Allars 1997). Procedures for the independent review of administrative decisions by a specially constituted court (Aronson and Dyer 2000), the institution of an Ombudsman with investigative powers who can hear complaints by individual citizens (Caiden 1983), and freedom of information legislation which provides public access to government documents (Birkinshaw 1997) are three elements of an administrative law system which can contribute to the integrity of governments.

Specialised bodies for the investigation and prosecution of serious economic crime

In many nations, the investigation of complex and sophisticated economic crime lies beyond the capacity of conventional law enforcement agencies. Some have thus created new agencies with special powers and expertise to address specific issues. The Independent Commission Against Corruption in Hong Kong, the Serious Fraud Office in the United Kingdom, and their variations elsewhere, are all examples of such agencies. This is not to suggest that specialised bodies are essential to resolving all problems in all jurisdictions. Where more general law enforcement bodies are adequate, there may be no need to create new ones. Indeed, a proliferation of agencies may lead to overlap and duplication, to bureaucratic rivalries, and to important cases 'falling between the cracks'. The effective exchange of intelligence and operational information can be made difficult. Such lack of cooperation may often be to the advantage of offenders, who may be able to delay or avoid detection and prosecution through a lack of coordination on the part of law enforcement agencies. However, the increasing specialisation of economic life suggests that designated organisations may be appropriate in some circumstances.

Cash transactions reporting

The challenge of money laundering and tax evasion is made much easier when the offender is able to shift funds around undetected. To this end, a growing movement among nations around the world has seen the development of cash transaction reporting systems. Banks and other financial institutions are now required to report all transactions over a specified amount to a central authority, or any transaction of any amount which appears in some manner to be suspect. In those jurisdictions where cash transaction reporting systems are in place, it becomes that much easier to 'follow the money trail'.

A free press

The famous adage that sunlight is the best disinfectant has already been noted. To the extent that an open and free press exists within a nation, questionable practices will be subject to questioning. This is important across a range of offences, from bribery and corruption to consumer fraud and fraud against shareholders and directors. This is not to suggest that the media are always virtuous and responsible in their coverage.It could be said, however, that the best antidote for irresponsible speech is more speech.

An adequate regulatory system

Freedom of expression does not extend to the freedom to publish false or misleading advertising or spurious commercial claims. A regulatory system

which can identify such misconduct and respond to it effectively will help ensure the integrity of markets is maintained. This need not be the exclusive province of government. Private remedies such as civil litigation, and self-regulatory regimes by individual companies and industry associations, are no less important than government agencies. A regulatory system which combines private and public remedies is likely to be more effective than one based solely on government or on self-regulation.

Mechanisms for building public awareness

By no means should knowledge about fraud and fraud risks remain a monopoly of law enforcement agencies. Because the first line of defence against fraud can and should be self-help, appropriate knowledge should be shared with private citizens, businesses and public sector agencies. All prospective victims of fraud—and this includes almost everyone—should be aware of the types of fraudulent activity to which they are most vulnerable, the 'red flags' or *indicia* of fraud, the most appropriate means of prevention, and best avenues of response when they detect an offence. New developments in communications permit not only the dissemination of basic fraud control information, but also the reporting of suspicious activity to appropriate authorities. The internet abounds in materials on fraud control; some industry-specific, others focusing on certain vulnerable groups such as senior citizens. Other sources of information are medium-specific—sites are dedicated to warning of fraud on the internet. Moreover, many law enforcement and regulatory agencies have established hotlines which are available to fraud victims or civic-minded third parties to report illegal or questionable conduct.

Freedom for individuals to form non-government organisations

Some of the most effective actions to combat economic crime are implemented by citizen groups. Before the rise of the modern state, citizens performed a number of functions (including policing, prosecution and imprisonment), which later became functions of government. Even in modern times, citizens' groups undertake activities that complement the work of government agencies. Two examples are victim assistance and prison aftercare associations. The control of corruption is facilitated by organisations such as Transparency International. Consumer groups and Better Business Bureaus remain vigilant against unfair trading. Citizens' crime commissions are vigilant against activities as diverse as abuse of power by law enforcement agencies, bribery and electoral fraud.

Responsible banking

In addition to their role in the prevention of money laundering, banks and other financial institutions have an important role to play in the prevention

and control of economic crime. Prudent lending practices will deny opportunities to the unscrupulous. The challenge facing governments today is to allow sufficient flexibility in the financial services industry to permit the economy to flourish, but to provide sufficient safeguards to protect against irresponsible or predatory conduct.

Commercial third parties

A variety of other third parties can complement the work of governments in the prevention and control of economic crime. A burgeoning industry in information security can assist clients in the public and private sectors to ensure the integrity of their systems. All of the large multinational accounting firms offer fraud control services to clients anywhere in the world. Many have established departments or subsidiaries specialising in fraud prevention. Their products range from a total review of risk management practices to more narrowly focused issues such as security of information technology systems.

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

Market forces themselves may exert positive effects from time to time on the behaviour of some public and private organisations. There are opportunities for the second-order operation of market forces through the guidance provided by financial and insurance institutions, and by institutional investors.

Open political system

An open political system permits individual citizens, interest groups or an organised opposition the freedom to question policies and programs. A viable political opposition can be alert to financial irregularities in the public and private sectors and can make them more difficult to conceal.

International cooperation

Because many fraud offences do not involve face-to-face interactions in their commission, it is possible for offenders and victims to be located in more than one jurisdiction. More sophisticated conspiracies may involve individuals in three or more jurisdictions within Australia or overseas. Few remedies are available to the unfortunate individual who might fall victim to such activities. The transnational dimension of many economic crimes requires unprecedented multilateral international cooperation, from formal treaties and mutual assistance arrangements to informal liaison between and exchange of law

enforcement personnel. Transnational electronic crime will require very timely cooperation, involving the capability of contacting overseas authorities at a moment's notice.

Sanctioning of offenders

While some would argue that severe penalties do not always deter crime, or that increasing penalties is unlikely to achieve a commensurate decrease in crime, one should not ignore the potential usefulness of punishment for economic crime. Economic crime is often based, to an extent greater than in other areas of crime, on rational decision making. Embezzlement does not occur in a moment of passion; corrupt payments are not made in an alcoholic rage. Penalties proportionate to the seriousness of the crime can send a message to would-be offenders, and educate the public that economic crime is serious and will not be tolerated.

Economic crime prevention

None of the solutions presented here is guaranteed to prevent economic crime, but each helps reduce the risk of such crime. The greater the number of preventative measures in place, the more difficult it is to perpetrate fraud and other forms of economic crime. It may be useful to use the analogy of a web. Any one strand of a web may be insufficient to support a load. But many strands, interwoven, may be very strong indeed.

The prevention and control of economic crime should not impose unrealistic burdens on commerce or on agencies of the state. Absolute integrity may be unattainable, and its pursuit may have counterproductive consequences. One might speak of 'burning the house to roast the pig'. It is ultimately the overall health of the economy and the integrity of its markets which are of greatest importance. Initiatives for the prevention and control of economic crime should be undertaken according to a risk-benefit calculus. This would see the most stringent controls operating where there is significant vulnerability to catastrophic loss, with fewer controls in place when risk is correspondingly less. The challenge for the future lies in implementing systems which will reduce opportunities for fraud, while at the same time allowing commerce to flourish.