possessed of an officer 'on the beat' in the not so distant past. At the Customs barrier, traditional methods of manual observation and drug-detecting sniffer dogs have been supplemented by 'Backscatter' X-ray technology, Ionscans and K910B Buster devices.[140] It is clear that such developments in the use of technology are a positive aid to crime control. The prospects for the future are limited only by human ingenuity, with cost reductions, miniaturisation and increasing connectivity offering the benefits of ubiquity and speed.

1.160 Equally persuasive is the argument that if the public and governments have an expectation that their law enforcers will investigate and bring to justice the perpetrators of serious crime, then they should be given access to the latest investigatory tools. Obviously adequate funding holds part of the answer - an area outside the Committee's area of interest. It can, however, give advice to governments about the adequacy of the legislative environment that they have created and in which their officers are expected to operate with maximum effectiveness.

1.161 This Chapter has highlighted the inconsistencies in the national legislative structure which act to thwart efficient law enforcement but which criminals are free to exploit. While in recent years Australian governments have achieved much for which they should be commended, with the development of CrimTrac the most notable example, the Chapter contains a clear call to the Commonwealth, State and Territory Governments to work together on achieving outcomes which are beneficial for all Australians, not simply parochial local interests.

1.162 With goodwill on all sides, positive progress was able to be made in the comparable area of the national regulation of corporations. Harmonisation of State and Territory laws does not require total uniformity, only consistency. That is indeed the basis on which the Committee can call for consideration to be given for TI to be devolved to the States on the one hand without being in contradiction on the other hand with its general proposition that cross-border differences should be eliminated in relation to surveillance device legislation. It may well be, therefore, that the national classification system holds a better precedent for a national law enforcement regime, where all parties have agreed to abide by common national standards, while individually retaining discretion over offence provisions at the State and Territory level. New and emerging technological developments raise many challenges. Governments must meet those challenges cooperatively and proactively.

---

140 See *Submissions,* pp. 202-3 and 241 for detailed descriptions. Mrs Marion Grant, the Australian Customs Service's National Manager, Border Operations, also informed the Committee that a cargo management re-engineering process was underway to make greater use of computer applications, including artificial intelligence systems, in its dealings with importers and exporters - see *Evidence,* p. 54.

CHAPTER 2

MONEY LAUNDERING AND ELECTRONIC COMMERCE

Introduction

2.1 The world has experienced significant economic, political and technological changes in recent years. We have seen a revolution in communications and transport; the deregulation of the financial systems and the development of global markets; and the breakdown of centrally planned economies and their replacement with market oriented ones. This has brought about a massive expansion of legitimate global trade in goods and services and, on the 'crime follows opportunity' principle, it has also facilitated the expansion of crime.

2.2 A regular concomitant of much crime, especially organised crime, is the attempt to legitimise its proceeds. Those proceeds are vulnerable to detection and, potentially, confiscation if they are not 'laundered' and made to appear respectable. Money laundering has come to be seen, not as a relatively victimless crime, but as a significant threat to the economy. As Australian Institute of Criminology researchers Peter Grabosky and Russell Smith described the situation:

> Money laundering is of great concern to law enforcement agencies, and for very good reason. A common strategy for concealing the proceeds of crime entails their investment in and commingling with the assets of legitimate business. The infiltration of legitimate enterprise by sophisticated criminals is a significant threat. Not only can legitimate business provide a convenient cloak or cover for further criminal activity, but the enterprise itself can be exploited and its assets stripped for personal gain, at the expense of investors and creditors. A nation's reputation for commercial honesty could be tarnished by criminal infiltration of legitimate business, with attendant consequence for its overall economic well-being. At the extreme, smaller economies can be seriously distorted by the infiltration of criminal assets, to the extent that the political stability of a smaller state may be threatened.[1]

2.3 Being of an entrepreneurial nature, organised crime seeks to use laundered money to sustain its further criminal activities, which is an added incentive to governments to attempt to prevent it.

2.4 Successive Australian governments have given considerable priority to anti-money laundering activities, as evidenced by the passage of the *Proceeds of Crime Act*

---

1 Grabosky, P. and Smith, R. *Crime in the Digital Age,* Federation Press, Sydney, 1998, p. 175.

1987, the then *Cash Transaction Reports Act 1988*[2] and the *Mutual Assistance in Criminal Matters Act 1987.* Money laundering became an offence in its own right in this country in 1987. Australia was a founding member of the Financial Action Task Force on Money Laundering (FATF), established in 1989 by the G7 group of countries. The NCA also conducted a major study into money laundering techniques in 1991, following a reference from the then Attorney-General.[3]

2.5 As the 1990s progressed, it became clear that the combination of global financial markets, networks for the electronic transfer of money, easy access to financial havens and banking secrecy laws in some countries had the potential to facilitate money laundering. At the request of the then Commonwealth Law Enforcement Board, the Australian Transaction Reports and Analysis Centre (AUSTRAC) formed the Electronic Commerce Task Force (ECTF) to work cooperatively with law enforcement agencies, industry, privacy groups and interested government bodies in identifying emerging electronic commerce issues of potential concern to law enforcement. The task force reported in November 1996[4] and, as noted in the Preface, this Committee's predecessor invited ECTF representatives to discuss the report's findings at a public hearing.

2.6 One of its recommendations was for the formation of an oversight body to handle Australia's entry into the information economy in a holistic manner. The National Office for the Information Economy was established in 1997 within the Communications, Information Technology and the Arts portfolio, with the brief to develop, oversee and coordinate Commonwealth Government policy on electronic commerce, online services and the Internet.

2.7 In July 1997 the Attorney-General set up an Electronic Commerce Expert Group (ECEG) to consider the legal impediments to electronic commerce within the framework of international standards and to report on the form and scope of arrangements for the regulation of e-commerce. Its report was presented in March 1998.[5]

2.8 Technological developments moved so swiftly that a Research Group on the Law Enforcement Implications of Electronic Commerce (RGEC) under the aegis of AUSTRAC was commissioned by the Heads of Commonwealth Operational Law Enforcement Agencies in 1997 to take up where the ECTF left off. In 1999, RGEC produced three reports which have been of inestimable value in shaping the

---

2 In 1991, the Cash Transaction Reports Amendment Act replaced the word 'cash' with 'financial'; the Act is hereafter referred to as the Financial Transaction Reports Act ('the FTR Act').

3 NCA, *Taken to the Cleaners: Money Laundering in Australia,* AGPS, Canberra, 1991.

4 Electronic Commerce Task Force, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board,* AUSTRAC, West Chatswood, 1996.

5 ECEG, *Electronic Commerce: Building the Legal Framework* Canberra, 1998.

Committee's thinking on these issues.[6] RGEC has now become the Action Group on the Law Enforcement Implications of Electronic Commerce (AGEC) because it is now charged with putting the results of its research into action.[7]

2.9 In other initiatives, the annual Australasian Police Commissioners' Conference has been active in its efforts to coordinate a national law enforcement approach. It resolved that a National Fraud Desk be established as a secure intranet web site on the ABCI's ALEIN database, which provides law enforcement with up-to-date information on emerging trends and new techniques. It also agreed to establish an Electronic Crime Steering Committee, supported by an Electronic Crime Working Party, to evaluate Australia's capacity to respond to e-crime.[8] In 2000, the Working Party produced a comprehensive scoping paper, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* which the Committee has drawn on considerably in considering appropriate law enforcement strategies for dealing with electronic crime.

2.10 In this Chapter, the Committee will address the broad issues related to money launderering, including the techniques used and the local and international law enforcement arrangements to combat it. It will also consider the development of electronic commerce, its characteristics, level of regulation and potential for abuse. Finally, the Committee will consider the potential for money laundering through e-commerce and whether additional law enforcement measures need to be considered.

Money laundering

Definitions

2.11 Put simply, money laundering is 'the processing of criminal proceeds in order to disguise their illegal origin'.[9] A more elaborate definition is offered in the *Proceeds of Crime Act 1987* (Cth):

> A person shall be taken to engage in money laundering if, and only if:
>
> - the person engages, directly or indirectly, in a transaction that involves money, or other property, that is proceeds of crime; or
>
> - the person receives, possesses, conceals, disposes of or brings into Australia any money, or other property, that is proceeds of crime and the person knows, or ought reasonably to know, that the money or other property is derived or realised, directly or indirectly, from some form of unlawful activity.[10]

---

6 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* West Chatswood, 1999.

7 Ms Elizabeth Montano, AUSTRAC Director, *Evidence*, p. 31

8 AFP, *Submissions*, p. 60.

9 FATF, *The Forty Recommendations*, OECD, Paris, 1990, p. 1.

10 *Proceeds of Crime Act 1987 (Cth),* s.81(3).

Background

2.12 Narcotics trafficking has traditionally been regarded as the single largest source of criminal proceeds.[11] And, as the ABCI points out, illicit drugs and cash are inextricably linked,[12] so the 'proceeds' have usually been in the form of cash.

2.13 In the early days, laundering was achieved by such techniques as 'smurfing', where couriers were employed to go to a large number of financial institutions in order to convert relatively unobtrusive amounts of cash into bank cheques or overseas funds transfers, thereby avoiding the attention which might otherwise have been drawn to a single, substantial cash transaction. Alternatively, the cash was moved out of the country by cash couriers or transmitted via underground banks.[13]

2.14 In its 1991 study into money laundering techniques, the NCA found that the areas most used by money launderers were financial institutions, particularly banks, real estate, and company structures, including cash businesses. Solicitors were used to develop or assist in many money laundering schemes and to send proceeds of crime overseas, particularly to tax havens.[14]

2.15 The NCA study also outlined the most commonly used methods for laundering money at that time. Property or other assets could be purchased in a false name or through a company, purchased for less than their worth, or 'rented' to the money laundering owner. Funds could be deposited into, or moved through, accounts in false names. Funds could be sent overseas by telegraphic transfer, bank draft, travellers' cheques, or physically carried out of the country. Fake deposits could be made, loans to a business owned by the money launderer, or fake debts could be generated. Or funds could be passed through business structures in order to make them appear to be part of legitimate business activity.[15]

2.16 While all of the above techniques are likely to still be practiced, it appears that banking systems, both regulated and underground, remain highly significant vehicles for money laundering.

2.17 Underground banking systems such as 'hawala', 'hui' or 'hundi', 'fei ch'ien' and others have existed for centuries, particularly in Indian, Pakistani, Chinese and east Asian communities throughout the world. They operate on trust. A person wishing to transfer money or value deposits it with the 'banker' (often an ordinary trader) and arranges for its redemption, minus a commission, at an agreed-upon location which is often the business premises of an associate or close relative of the 'banker'. The actual

---

11 FATF, *Annual Report 1999-2000*, Paris, 2000.

12 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 104.

13 Grabosky, P., *Computer Crime in a World Without Borders,* Paper presented to the 70th Conference of Commissioners of Police of Australasia and the Southwest Pacific Region, Canberra 13 March 2000.

14 NCA, *Taken to the Cleaners: Money Laundering in Australia,* AGPS, Canberra, 1992.

15 ibid., p. ix.

assets need not physically move from country to country, unless required for balancing the books. Such systems are quite legal and are used for legitimate funds transfer, which makes it particularly difficult and culturally heavy-handed to crack down on them. They do, however, have a role to play in money laundering though, by the very nature of that practice, its extent is unknown.

2.18 Australia's multicultural population has ensured that it is an attractive host for such alternative remittance systems. An NCA investigation in 1999 uncovered one such system, operating from retail fabric shops in Melbourne. For a fee, money was transferred between Australia and Vietnam by telegraphic transfer purchased with cash or cheques or via telegraphic transfer via trading companies in Hong Kong and Vietnam.[16]

2.19 The accepted wisdom regarding money laundering suggests that it involves three stages: placement, layering and integration. Placement involves introducing the tainted proceeds into a legitimate context, such as a bank account, without revealing the source of the funds; layering involves moving the assets in a series of transactions to conceal their real ownership and location; and integration involves blending the funds into the mainstream economy, eliminating any indication of tainted origins.[17]

2.20 The initial 'placement' stage is critical for law enforcement authorities, because it presents the best opportunities for detection. Bank accounts still appear to be used by criminal groups to deposit money, often in parcels of less than $10,000,[18] which is the cash transaction reporting threshhold under the FTR Act. The funds are then transferred to overseas accounts, then channelled back into Australia as 'loans' to businesses connected to the launderers. 'Layering' can be achieved by the successive rerouting of funds between bank accounts and corporate structures, which can give the impression of substantial business activity, and is a practice facilitated by the speed of the Internet. 'Integration' will be assisted by the development of stored value systems or electronic cash, to which funds can be downloaded from institutional sources.

2.21 In a recent report on money laundering, the FATF found that these methods continued to be used, along with currency smuggling across borders, the use of such professionals as insurance or securities brokers to assist in laundering schemes, and the use of real estate, gambling, legitimate remittance services and trusts. The international trade in goods and services is also used, both as a cover for money laundering or as a money laundering mechanism itself, by over- or under-valuing goods.[19]

2.22 Emerging trends in money laundering in 1999-2000 in Australia included stock market manipulation, or share ramping. The funds for such transactions are sent

---

16 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, p. 108.

17 Grabosky P. and Smith R., *Crime in the Digital Age,* Federation Press, Sydney, 1998, p. 175.

18 This offence is known as 'structuring'.

19 FATF, *Annual Report 2000-2001,* OECD, Paris, 2001, pp. 15-17.

offshore then repatriated to purchase Australian securities. One case investigated by the NCA involved a Chinese student suspected of laundering money for a narcotics syndicate by using fellow students to remit funds overseas by telegraphic transfer in amounts of less than $10,000.[20]

2.23 The correspondent banking system seems to be increasingly used in money laundering and since the mid-1990s a large number of financial institutions have been registered in offshore tax and financial havens in the Carribean and the Pacific islands. The Cook Islands, for example, with a population of 18,000 is reportedly home to some 3000 separately registered offshore trusts, 1200 registered offshore companies and seven offshore banks; Nauru has some 400 licenced offshore banks; Samoa features 15 offshore banks.[21]

The extent of money laundering

2.24 By its very nature, money laundering is a covert activity, all but impossible to quantify. An effort was made in 1995 when AUSTRAC commissioned Mr John Walker, an independent consultant criminologist, to analyse it. His conclusions were that between $1000 million and $4500 million of Australian proceeds of crime are laundered within Australia or sent overseas. As much as $5500 million may be being sent out of Australia to overseas tax havens, some of which would be from Australian crime and some being overseas crime laundered via Australia, and as much as $7700 million brought to Australia for laundering.[22]

2.25 A 1998 estimate by Mr Michel Camdessus, former Managing Director of the International Monetary Fund, was that between two and five per cent of global GDP would be a consensus range for money laundering worldwide.[23] The Director General of Interpol, Mr Raymond Kendall, had suggested to the Committee in late 1996 that some $450 billion was being laundered per annum worldwide. The need for international action to address illicit activity of this magnitude is apparent.

Domestic anti-money laundering initiatives

2.26 Traditional law enforcement and regulatory attention tended to be directed to the predicate offence, such as the fraud, the drug dealing or the tax evasion. But the value of following the money trail was soon realised, resulting in the passage of the FTR Act.

2.27 The FTR Act requires cash dealers, solicitors and members of the public to report particular financial transactions to the Director of AUSTRAC. Cash dealers are defined broadly to include financial institutions such as banks and building societies,

---

20 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 108.

21 FATF, *Review to Identify Non-Cooperative Countries or Territories,* Paris, 22 June 2001.

22 Walker, J., *Estimates of the extent of money laundering in and through Australia,* AUSTRAC, Sydney, 1995, p. 41.

23 ABCI, op.cit., p. 105.

insurance companies, futures brokers, managers of unit trusts, firms that deal in travellers cheques or money orders, remittance dealers, casinos, bookmakers and totalisator agency boards. Under the FTR Act cash dealers must report transactions of $10,000 or more, or foreign currency equivalents; they must report all international funds transfer instructions; and they must report any suspicious transaction. Additionally they are required to verify the identity of persons who open accounts or become signatories to accounts. The FTR Act prohibits the opening of an account in a false name. Solicitors are required to report cash transactions of $10,000 or more, while members of the public must report movements of currency of $10,000 or more, into or out of Australia.

2.28 Recent proposed amendments to the FTR Act in Schedule 6 of the *Measures to Combat Serious and Organised Crime Bill 2001* (currently under consideration by the Senate Legal and Constitutional Legislation Committee) extend the definition of cash dealer to include real estate agents and currency dealers, who are potential money laundering channels not currently included under the Act's reporting requirements.

2.29 With funds provided under the National Illicit Drug Strategy, AUSTRAC in 1999-2000 undertook a high risk cash dealer strategy, targetting remittance dealers, bullion sellers and money exchangers. Its audit team conducted 69 audits of such dealers, discovering many instances of non-compliance with the FTR Act in respect of international funds transfer instructions.[24] Just as importantly, such enforcement campaigns also encourage higher levels of compliance in future.

2.30 The number of suspect transaction reports received by AUSTRAC from cash dealers in 1999-2000 was 7,085, a rise of some 500 over the previous year. The majority of reports came from banks, with a small and decreasing number from credit unions, casinos, issuers of travellers cheques and other cash dealers.[25] Analysis of the reports showed that the majority related to tax evasion. Next in numerical significance was structuring, followed by 'unusually large cash transaction', then money laundering, with in many cases the activities being interrelated.

2.31 Suspect transaction reports may, of course, prove to be legitimate activities upon investigation. Nevertheless, AUSTRAC reported that in 1999-2000 the law enforcement agencies to which it reported suspect activity used the information in at least 628 investigations. Uses to which the information was put included: revealing the identities of previously unknown persons and providing links to known entities; confirming addresses; showing associations between targets; analysing movement within Australia and links with overseas countries; and determining the size of criminal enterprises.[26] In the sample cases provided, AUSTRAC's financial intelligence proved particularly useful in tax evasion, narcotics trafficking and people smuggling cases.

---

24 AUSTRAC, *Annual Report 1999-2000,* West Chatswood, 2000, pp. 52-53.

25 ibid., p. 59.

26 ibid., p. 74.

2.32 At the time of the NCA's establishment in 1984, money laundering was not a criminal offence in Australia, it was not illegal to operate bank accounts in false names, there was no Commonwealth or State proceeds of crime legislation and there was no financial transaction reports legislation in Australia. Its legislation was silent on its capacity to investigate money laundering as a 'relevant offence' and its investigations into money laundering were necessarily in conjunction with a predicate offence.

2.33 During the ensuing 17 years of its operations there have been significant changes to the law and administrative practices in Australia relating to money laundering, and the NCA has adapted its role and functions accordingly. In October 1994 the NCA established the Agio Task Force to coordinate the efforts of Commonwealth and certain State law enforcement agencies in the investigation of financial intelligence of suspected money laundering and related criminal activity. In May 1994 the Commonwealth granted the NCA the first of its Limbeck references which enabled the Authority to use its coercive powers to add value to the intelligence information.

2.34 Since July 1997 Commonwealth references - known as Operation Swordfish - have been granted to the NCA to investigate organised revenue fraud (tax evasion, Customs duty and excise evasion), money laundering and predicate offences, including drug trafficking. The *National Crime Authority Legislation Amendment Bill 2000*, currently being considered by the Parliament, includes a proposal to include money laundering as a 'relevant offence' in the NCA Act, which would enable the NCA to apply its special powers directly to such offences in their own right, rather than as an adjunct to another relevant offence.

2.35 Another NCA initiative has been the establishment of a Profits of Crime Case Studies Desk using Intranet technology provided through the ABCI's ALEIN network. Case studies of money laundering and investigative techniques are thus able to be shared among Australian law enforcement agencies.

2.36 The other major stance Australia has taken is to legislate to confiscate the illicit proceeds of convicted criminals, through the *Proceeds of Crime Act 1987* [the POC Act]. While certain fine tuning has taken place, it was recognised that a more major overhaul might be needed to ensure that the basic objectives of the legislation were being met and to comply with Australia's international obligations, including under the Council of Europe *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. A review of the POC Act was referred to the Australian Law Reform Commission, which produced a report, *Confiscation That Counts,* in 1999, recommending, inter alia, a civil forfeiture regime. In its submission to the Committee, the National Crime Authority was strongly supportive of this recommendation.[27]

---

27 *Submissions,* p. 174.

2.37 On 20 July 2001 the Minister for Justice and Customs, Senator the Hon Chris Ellison, issued an exposure draft of a proposed Proceeds of Crime Bill 2001, which incorporates a civil, or non-conviction based, forfeiture of proceeds of crime. The Minister also indicated that an associated bill would cover revised anti-money laundering offences.

International anti-money laundering action

2.38 The need for international cooperation in the fight against drug trafficking and concomitant money laundering was recognised early in the 1988 Vienna Convention (the United Nations *Convention Against Illicit Traffic in Narcotic and Psychotropic Substances*) and in the 1988 Basle *Statement of Principles* (of the Basle Committee on Banking Regulations and Supervisory Practices on the prevention of criminal use of the banking system for the purposes of money laundering).

2.39 It was the establishment of the Financial Action Task Force on Money Laundering (FATF) in 1989, however, that marked a significant step in international anti-money laundering action. As considered in more detail in Chapter 3, the FATF was established by the then G7 group of countries. It is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering. Such policies aim to prevent proceeds of crime from being utilised in future criminal activity and from affecting legitimate economic activity. Australia was a founding member of FATF; it was also instrumental in the setting up of a FATF-linked regional group, the Asia/Pacific Group on Money Laundering, in 1997.

2.40 In 1990, 40 FATF Recommendations were drawn up to cover all relevant aspects of the fight against money laundering; they were revised and updated in 1996. The 40 Recommendations set out the basic framework for anti-money laundering efforts and are designed to be of universal application. They cover law enforcement and the criminal justice system, the financial system and its regulation, and international cooperation. The recommendations are broad principles for action, for countries to implement according to their particular circumstances and constitutional frameworks. All member countries have their implementation of the 40 Recommendations monitored through a self-assessment exercise and through an on-site examination.

2.41 When the 40 Recommendations were first issued, the focus of many of their preventative measures was on detecting money laundering at the cash proceeds stage. This is reflected in the FTR legislation, which emphasises the reporting of cash transactions of over $10,000. A recent FATF meeting found that, e-commerce notwithstanding, 'cash remains the major if not primary form in which illegal funds are generated today' despite an ever-decreasing reliance on cash by the general public.[28]

28 FATF, *Report on Money Laundering Typologies 2000-2001,* OECD, Paris, 2001.

2.42 The United Nations has also been active in this area. At the 20th Special Session of the General Assembly on the World Drug Problem in June 1998, it adopted a *Political Declaration* and *Action Plan against Money Laundering*, which condemned the laundering of money derived from illicit drug trafficking and other serious crimes and urged all States to implement the provisions against money laundering in the United Nations *Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances* of 1988 and other relevant international instruments. Those provisions included:

- the establishment of a legislative framework to criminalise money laundering through confiscation of the proceeds of crime; and to encourage international cooperation and mutual legal assistance;
- the establishment of an effective financial and regulatory regime to deny criminals and their illicit funds access to national and international financial systems, through customer identification and verification requirements; mandatory reporting of suspicious activity; and removal of bank secrecy impediments; and
- the implementation of law enforcement measures to assist in the detection, investigation, prosecution and conviction of money launderers.[29]

2.43 In 2000 the UN finalised an *International Convention Against Transnational Organised Crime* which requires, among other things, signatories to establish comprehensive money laundering offences under their domestic laws and to adopt detailed measures to combat money laundering.

Electronic commerce

Definitions

2.44 Electronic commerce, or e-commerce, has been defined most simply as 'the use of computers and electronic communications networks to do business'.[30] Every type of business transaction in which the participants prepare or transact their business electronically can be regarded as e-commerce. Some have defined e-commerce more broadly still. The Sacher Group report to the OECD stated:

> Electronic Commerce refers generally to all forms of commercial transactions involving both organisations and individuals, that are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may have on the institutions and processes that support and govern commercial activities. These include organisational management, commercial negotiations and contracts, legal

29 www.austrac.gov.au/text/recent_news/international_money_laundering/index.htm, visited 27 July 2001.

30 National Office for the Information Economy, *E-Commerce for Small Business,* www.noie.gov.au/projects/ecommerce/SME/index.htm as at 1 May 2001.

and regulatory frameworks, financial settlement arrangements, and taxation, among many others.[31]

Background

2.45 E-commerce as we know it today has burgeoned since the mid-1990s, initially with business-to-business transactions, but now business-to-consumer transactions are taking off.

2.46 This growth has been made possible by the development and rapid uptake of the Internet. Access to Internet services is typically provided by an Internet Service Provider (ISP), a retailer who usually buys wholesale capacity from a telecommunications carrier. While corporate consumers generally connect to the Internet via a data line, residential users can access the Internet via a number of technologies including analogue dial-up, broadband and Wireless Application Protocol (WAP). Dial-up access over the public switched telephone network remains the most common. The computer, telecommunications and broadcast media that can be used to provide mass Internet access are rapidly converging, and thus represent some interesting regulatory challenges for the future.

2.47 E-commerce has the potential to offer many advantages over more traditional commerce, although its use is not without downside risks, as this Chapter discusses. It can empower consumers, giving them more information on which to base their purchase decisions, more choice in their source of supply and a greater ability to demand customised goods and services, and enabling them to conduct their transactions from home. For retailers, it can open up new business opportunities globally and benefits in terms of cost savings.

2.48 The government has signalled its support for e-commerce and made it clear that both e-commerce and the electronic delivery of public services are key strategic areas to be pursued. In December 1997, the Prime Minister responded to the *Investing in Growth* report with a statement committing the Commonwealth government to moving all appropriate Government services online by June 2001.[32] The passage of the *Electronic Transactions Act 1999* ensured that there was no legal impediment to the use of electronic communications to satisfy obligations under Commonwealth law.

Level of e-commerce

2.49 Growth in the most common prerequisite for e-commerce, connection to the Internet, is taking place rapidly. At the end of December 2000 there were 3.9 million Internet subscribers registered in Australia, of whom 3.4 million were household subscribers and 512,000 'business and government'. Together they downloaded 1,050

---

31 Ad Hoc Group of High-Level Private Sector Experts on Electronic Commerce, *Electronic Commerce:Opportunites and Challenges for Government,* OECD, Paris, 1997, p. 20.

32 Attorney-General's portfolio, *Submissions,* p. 195.

million megabytes of data.[33] Forty-six per cent of adult Australians accessed the Internet during the year to May 2000, compared to 41% a year earlier; 33% of households had home access to the Internet in May 2000 compared to 22% in May 1999.[34] Not surprisingly, capital city statistical divisions accounted for the majority of subscribers (74 %); only one per cent of subscribers accessed the Internet via points of presence in remote or very remote regions in Australia.

2.50 Internet access was provided by 696 ISPs at December 2000, down three per cent over the previous quarter, suggesting some rationalisation in the industry. Six very large ISPs, with more than 100,000 subscribers, provided access to 53 % of all Internet subscribers in Australia. Web hosting services were provided by 93 % of ISPs; 49 % provided secure access transaction capabilities. Of the 97,165 business and government web sites, 4,233, or 4 %, provided an environment for secure transactions.[35]

2.51 According to the ninth Australia Online Survey, 46 % of regular Australian Internet users, or 1.6 million people, have tried online shopping in the 12 months to September 2000, with nine per cent of those online shoppers having purchased online more than ten times.[36] In the second half of 2000, Australian retailers captured 68 % of the Australian online spend, up from 45 % in the equivalent period of the previous year. Books remain the most frequently purchased online product, while food and groceries are the clear leaders in repeat online purchases. Sales of CDs, videos, travel and concert or event ticket purchases are building up.

2.52 Other commercial uses of the Internet are increasing: in December 1998, for example, 12 % of regular Internet users participated in Internet banking; by December 2000 that figure had reached 51 %.[37]

2.53 The survey also found that, in December 2000, almost half the regular Australian Internet users had been online for less than two years. The evidence suggests that the levels of participation in Internet transactions such as shopping and banking are heavily influenced by the length of a user's Internet experience, with higher value online transactions not being undertaken in the first two years of Internet use.[38]

2.54 The regular Internet users surveyed continued to express much the same concerns with the Internet as had been shown in previous surveys: computer viruses (22%); response times (13%); security of financial transactions (12%); junk email or

---

33 Australian Bureau of Statistics, *Internet Activity, Australia,* December quarter 2000, Cat. no. 8153.0

34 Australian Telecommunications Authority, *Telecommunications Performance Report 1999-2000,* ACA, Melbourne, 2000, p. 161.

35 Australian Bureau of Statistics, *Internet Activity, Australia,* December quarter 2000, Cat. no. 8153.0.

36 www.consult, *The 9th Australian Internet User Report, July-December 2000,* p. 30.

37 ibid., p. 34.

38 ibid., p. 7.

intrusive marketing (12%); privacy (11%); and cost of Intenet access (10%). When asked what would reassure them about online transactions, 21% indicated that 'guarantees' from banks and retailers regarding transaction security would be helpful.[39] Of the non-purchasers online, 35% gave as their reason that they did not trust the Internet with their credit card details. The online purchasers did so for a variety of reasons: 29% cited convenience; 13% to save money; 13% to buy goods unavailable in Australia; and 10% to save time.[40]

2.55 Statistics from the United States show that almost 20 million US households shopped online in December 2000, spending in total US$6.1 billion, with the average per household spend US$308.[41] Forrester Reseach estimates that worldwide net commerce will rise from US$657 billion in 2000 to $6.8 trillion in 2004, with the Asia-Pacific region accounting for about a quarter of that figure.

Features of e-commerce

2.56 E-commerce has a global spread, it is open to all with an Internet connection, it is convenient, and it is immediate. One can pick and chose from a vast array of goods and services from all around the world, compare prices and quality, and effect a purchase with the click of a mouse from the comfort of home, 24 hours a day, seven days a week. Transactions occur in real time, with the vendor being paid immediately

2.57 But e-commerce has other features which are more challenging. It uses the Internet, an unregulated medium, broadly speaking, and one which has attracted a new breed of offender, the cyber-criminal. Its success is reliant on the use of cryptography to ensure the security of financial transactions. It removes the certainty of knowing who you are dealing with, for both purchaser and vendor. And it means that your private details are more widely known than before.

2.58 E-commerce has the potential to bring about change on an unprecedented scale. In this report, the Committee will not consider matters such as the impact of e-commerce on the economy as a whole, nor its social or political ramifications, important though they may be. It will concentrate on those features of e-commerce which may be susceptible to crime, including money laundering, and consider the implications for law enforcement.

E-commerce challenges and responses

2.59 E-commerce is expanding at an exponential rate. This suggests that for the present, both purchasers and vendors are sufficiently convinced of its relative security or, at the least, reassured that the benefits outweigh the possible risks. Those risks relate primarily to the medium of the Internet with its anonymity, speed and geographic spread, and include: the relative ease with which identity fraud can be

---

39 ibid., p. 44.

40 ibid., p. 47.

41 Forrester Research Online Retail Index, www.forrester.com

perpetrated; the likelihood of external hacking, denial of service or spamming attacks to e-commerce web sites; the authentication of e-commerce web sites; the concealment of communications with cryptography; and the security of payment systems. Many of the core issues are not unique to the electronic world, but may present new challenges in that context, and require different responses. The Committee examines these features in the following sections.

Geographic spread

2.60 When things go wrong, e-commerce may present jurisdictional challenges because of its global spread. Consumer protection laws vary greatly from country to country and it might be impossible to locate an organisation comparable to Australian fair trading or consumer affairs bodies to assist.

2.61 A typical scenario might be as follows. Australian company XXX establishes a commercial web site in the USA, for faster access and lower costs. It advertises widgets, with an extensive online catalogue and online payment facilities. It software accesses backend supply databases in London, Rome and Buenos Aires, and it has arrangements with couriers to deliver its widgets anywhere in the world. The companies whose credit cards XXX accepts issue invoices to its participating banks from regional headquarters in, say, Malaysia.

2.62 Such a convoluted scenario is the norm in e-commerce. When and if criminal conduct occurs along the way, interesting legal questions are raised. If, for example, in the scenario above, a New Zealand customer orders and pays for 100 widgets and fails to receive them because they are stolen somewhere en route, where does the offence take place? Which jurisdiction is responsible for dealing with it? What laws, if any, cover the offence in the jurisdiction in which it occurred? What evidence of the transaction is available and is it acceptable to the relevant court? In some circumstances, but not all, law enforcement agencies may be able to assist victims through recourse to mutual assistance arrangements (as described in Chapter 3) but for low-level offences assistance is unlikely to be a law enforcement priority.

2.63 The question of jurisdiction has been actively canvassed at international level. In particular, the Council of Europe *Draft Convention of Cyber-Crime* is a significant step towards the harmonisation of laws relating to computer-related crime, addressing as it does the substantive criminal law, search and seizure of electronic data, jurisdiction and mutual assistance.

Speed

2.64 E-commerce can be conducted instantly. For the private purchaser, this is one of its attractions; for the vendor, it may present problems especially in the automated sales area or inventory-and-dispatch systems. While most vendors employ automated scanning and verification procedures, they may not detect high-volume, low-value frauds which can be speedily effected on the Internet.

2.65 The Internet, with its multiplier effect, facilitates email spam and denial of service attacks, in which thousands of emails can be routed through a third-party server for distribution worldwide. When directed at an e-commerce site, the damage can be dramatic.

2.66 These are the risks involved in participating in e-commerce and should be managed as such. High-level preventative IT security is an obvious answer for the private sector, rather than reliance on law enforcement assistance.

Anonymity

2.67 In traditional business dealings, customers build up relationships over time with retailers where familiarity, experience and a bricks-and-mortar presence all added to the security of business dealings. But a feature of e-commerce is that of separation. Buyer and seller may never meet in the real world and have no direct means of knowing who they are really dealing with. While the loss of face-to-face contact and the resultant loss of collateral information introduces an element of risk into e-commerce transactions, it is important to remember that mail order and telephone order transactions, with not dissimilar features, have been in operation successfully for some years.

2.68 Anonymity can be further enhanced by the use of anonymous remailers. As the name suggests, these are e-mail servers which strip off e-mail headers and onforward the message to the intended recipient, either anonymously or, if a response is required, with a pseudonym. Some remailers provide encryption services in addition to mail forwarding. And users who do not trust the remailers can of course forward their messages through multiple remailers. It has been suggested that remailers can batch messages so that, if a law enforcement agency intercepted them, it would not be able to deduce who was talking to whom.[42]

2.69 It is of course possible, in the investigation of potentially criminal conduct, for law enforcement to trace, with the assistance of ISP records, the Internet address or domain name from which a particular message was sent, and to discover the name of the person responsible for maintaining that domain name, but not to identify the user at the time.

2.70 The issue of identity is complicated because it is technically possible for a fake web site to masquerade as another, a practice known as 'spoofing'.[43] Individuals too can mask their identity by 'looping' and 'weaving' through a number of previously compromised systems.

---

42 Denning, D. and Baugh, W.E. 'Hiding crimes in cyberspace', in Thomas D. and Loader B.D. (eds), *Cybercrime: law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 125.

43 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood, 1999, p. 42.

2.71 For e-commerce to succeed, one of the imperatives is for parties to transactions to be sure of the identity of the person or site they are dealing with. Cryptography, or the practice of transforming the contents of a message to a form that cannot be decoded by unauthorised persons, is the generally preferred solution. A commonly used form is public key cryptography, which works as follows. Person A wishes to send a secure message to person B, so firstly A encrypts the message with B's public key, then 'signs' it with A's private key. B receives the message which is notionally from A and verifies that it is from A by decrypting it using the only key which will do so, namely A's public key, then decrypts the contents using B's private key.[44]

2.72 Public key cryptography is readily available software and the use of digital signatures increases confidence levels in the authenticity of a transaction. Without a biometric component, however, there will always be an element of doubt. For the time being, biometric identifiers such as fingerprint recognisers or iris scanners are relatively expensive and have not gained widespread acceptance. This can be expected to change should commercial demand make it viable.

2.73 Public key cryptography is equally available to money launderers and other criminals as it is to those seeking merely to communicate securely and privately for commercial reasons. Given the strength of even the commonly available cryptographic algorithms (with key lengths of 128 bits or more) law enforcement agencies world-wide have sought legislative leverage to compel access to keys, rather than engage in expensive and time-consuming and, at times, fruitless efforts to 'crack' the encryption. This matter is further considered in Chapter 1.

2.74 While it is generally agreed that encryption poses a potential threat to law enforcement agencies, the Committee is not aware of evidence of the actual extent of its use by criminals in Australia. The FBI's Computer Analysis Response Team began collecting such data in April 1998 and by December of that year, only four per cent of forensic cases handled involved the use of encryption.[45]

2.75 In terms of the problem for e-commerce of anonymity, public-key based, crypto-secured digital identification should provide a high level of confidence in transactions, but it may not do a great deal to assist law enforcement agencies. Legitimate and illegitimate commerce can exist side by side. The computer networks of large organisations are generally protected by firewalls against external security breaches, but this also means that individual Internet users may be represented externally by a single Internet Protocol (IP) number, thus complicating the identification process unless firewall logs are kept. And even if it is possible to identify the physical location of a computer with a particular IP number, it may run a

---

44 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, pp. 42-43.

45 Denning, D. and Baugh, W.E. 'Hiding crimes in cyberspace', in Thomas D. and Loader B.D. (eds), *Cybercrime: law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 112.

multi-user operating system, with identification only possible if users have a separate login ID.

2.76 The Committee notes that at present, there appears to be no requirement for entities that trade electronically to identify themselves other than by their URL. The RGEC report noted that the Australian Taxation Office was unable to locate owners of 15 % of businesses with com.au domain names.[46]

Identity fraud

2.77 Knowing who you are dealing with electronically is further complicated by the ease with which a false identity can be achieved. As the Office of Strategic Crime Assessments (OSCA) has noted, technology has weakened the integrity of many identifiers currently in use.[47] False identity papers can be readily acquired through the Internet: a number of web sites offer near-authentic forgeries of official documents, which can in turn be used to facilitate money laundering and other crimes. The NCA expressed particular concern about the registration of business names in false identities, SIM cards and mobile phones in false names, and forged or false credit cards, and, while acknowledging the difficulties in verifying the authenticity of identification documents, it also expressed its concern at the apparent readiness of private and public sector bodies to accept identity documents at face value.[48]

2.78 Proof of identity is required in Australia for such commercial activities as opening a bank account or registering a company. Birth certificates are often required. The banks are acutely aware of the difficulties and have undertaken research into the extent of the problem. Westpac and the NSW Registry of Births, Deaths and Marriages undertook a pilot study of a certificate validation service, finding that some 13% of birth certificates provided as part of the identification documentation were false.[49]

2.79 The problem is compounded by the fact that once one agency accepts the false documentation and issues, for example, a driving licence or a company number, those readily verifiable details will assist the false identity holder to build up a portfolio of 'proofs'. Even the '100 Point' system of identity verification used by a range of Commonwealth agencies is vulnerable to abuse from the use of forged or stolen identity documents and such is the range and source of possible documents being presented that organisations' abilities to check are limited.

---

46 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 50.

47 OSCA, *The Changing Nature of Fraud in Australia,* Canberra, 2000, p.10.

48 NCA, in *Submissions,* p. 166.

49 House of Representatives Standing Committee on Economics, Finance and Public Administration, *Numbers on the Run,* 2000, p. 67.

2.80 The extent of the use of identity fraud is, by its nature, impossible to quantify. In one 1999 survey of 1800 large Australian companies, KPMG found that 11.9% of fraud incidents involved the use of false documentation.[50]

2.81 In one widely-reported American case, touted as 'the largest ID theft in Internet history', a Brooklyn busboy named Abdullah, using computers in a local library, duped companies into providing credit reports on more than 200 of the celebrities, millionaires and corporate executives listed in Forbes magazine. He then used the confidential data to clone their identities and gain access to their credit cards at accounts at some of the most prestigious brokerage houses and investment banks.[51]

2.82 While technology has augmented this problem, technological devices also offer perhaps the best prospect for limiting certain kinds of identity fraud. User identification systems which involve security devices incorporating unique biometric identifiers are already available: keyboards and mice containing fingerprint scanners, for example.[52] Space geodetic methods can be used to pinpoint the physical location of computer users. And single-use passwords, challenge-response protocols and call-back systems can also be used to carry out user authentication.

Security of payment systems

2.83 Another aspect of e-commerce which discourages potential online shoppers is the question of whether the payment system is secure. In Australian-based e-commerce, pre-existing credit arrangements such as credit and charge card schemes are still the most common payment form for purchases via the Internet, with purchasers quoting a card number, protected by encryption. These schemes, being global, facilitate international transactions involving currency conversions, but are capable of abuse: the payer can repudiate the transaction; and card numbers can be fraudulently obtained.[53]

2.84 The perception is that credit cards can be easily intercepted on the Internet and misused. This has certainly occurred. The ABCI told the Committee of numerous recent incidents of organised Asian criminal syndicates 'skimming' electronic data off legitimate credit cards and encoding the information on stolen or counterfeit cards, which are then used to purchase goods. An investigation in New South Wales, Operation Massat, resulted in the dismantling of a highly organised Malaysian based

50 ibid., p. 75.

51 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 5.

52 Grabosky P., Smith R. and Dempsey G., *Electronic Theft: Unlawful Acquisiton in Cyberspace,* Cambridge University Press, 2001, p. 195.

53 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 59.

syndicate involved in approximately $50 million counterfeit-related fraud in 1998 and 1999.[54]

2.85 It appears that much credit card fraud on the Internet comes from apparently valid credit card numbers generated by software programs. When the charges are small, the likelihood of full authorisation checks being performed is limited; checking would disclose that the card numbers were fraudulent.[55]

2.86 Research into credit card losses in the online retail industry has shown mixed results. ActivMedia found that 'chargebacks' amounted to only 1.22 %, as opposed to 1.47 % offline.[56] This is well within the average business risk most retailers would accept. Other reports have suggested otherwise, however. It has been reported that a website operated by Harvey Norman was shut down because a quarter of the orders placed on it were on stolen credit cards.[57] A UK report found that e-commerce firms were reporting up to 25% of online transactions as fraudulent, with an average of 5%.[58] Yet another source reported overall fraud rates of 0.08 to 0.09 %, with little difference between face-to-face and mail-order/telephone-order transactions and electronic transactions.[59] Whatever the exact level, it is clearly a matter which will self-regulate, with merchants refusing to accept credit card payments if they become too unreliable.

2.87 From the point of view of the customer, most financial institutions offer their customers a measure of protection against fraudulent use of their credit card. So long as the unauthorised transaction is reported immediately, banks will usually not hold the cardholder liable, or will limit liability. Similarly, if the goods fail to arrive or are returned because they are faulty, banks may reverse the payment to the business.

2.88 Credit card numbers or other payment details are encrypted before being transmitted over the Internet. Both Netscape Navigator and Microsoft Internet Explorer use a method known as Secure Sockets Layer (SSL) to encrypt data before transmitting it, and show a lock or an unbroken key in the browser window. But SSL does not serve to authenticate either transacting party.

2.89 The major card issuers and financial institutions have been developing a process to provide both advanced encryption, combined with a system of digital certificates provided by card issuers, known as Secure Electronic Transaction (SET).

---

54 *Submissions,* p. 127.

55 ACS & NOIE, *The Phantom Menace: Setting the record straight about online credit card fraud for consumers,* [2000].

56 ibid.

57 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 4.

58 ibid.

59 ACS & NOIE, *The Phantom Menace: Setting the record straight about online credit card fraud for consumers,* [2000].

SET would enable the identity of the cardholder and the merchant to be authenticated, while ensuring that neither the merchant nor the cardholder's bank sees the purchaser's credit card number. The RGEC report suggested, however, that SET was proving difficult to deploy.[60]

2.90 Given the level of concern about security of credit card payments, and the reluctance of some payees to accept payment by credit card because of the fees charged, alternative forms of payment, such as direct debit schemes, are developing. Many banks have begun providing Internet bill payment facilities, for example. A third method is the stored value scheme, by which purchasers pay for value in advance either on a smartcard or on a computer; the value is progressively depleted until it runs out and is topped up again.

2.91 The smartcard in particular was heralded as the replacement for cash for small purchases but has been slow to take off. It has been suggested that banks are reluctant to support stored value schemes for fear of losing fees from EFTPOS and credit cards, while merchants are either waiting for the critical mass to be generated to make the expenditure associated with implementing such schemes worthwhile or they are implementing private stored value schemes such as TAB accounts and pre-paid SIMs for mobile phones.

2.92 It has also been suggested that the smartcard future may depend on its adoption for multiple purposes, such as personal identification and access to services.[61] Both Germany and Spain have gone down this route, but Australia with its history of cultural aversion to the carrying of identity papers, as evidenced by the failure of the Australia Card proposal in the 1980s, is unlikely to follow suit.

2.93 There are Internet variations on the smartcard theme, variously called e-cash, Digicash or cybercash, where funds are deposited in a personal bank account and then transferred to the e-cash system which generates and validates e-cash for use on the Internet. The ABCI reported that only one Australian bank offered such a service.[62]

2.94 Internet payment schemes are in a state of evolution and it is difficult to predict which will become the norm. What is clear is that private stored value schemes operated by non-bank financial institutions outside the regulated financial sector could provide systemic risks for the financial sector.[63]

---

60 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 61.

61 Ad Hoc Group of Hi-Level Private Sector Experts on Electronic Commerce, *Electronic Commerce: Opportunities and Challenges for Government,* OECD, Paris, p. 36.

62 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 105.

63 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 63.

Computer system attacks

2.95 While e-commerce is dependent on the Internet, there is always a potential threat from computer network break-ins. The FBI has defined three types of cyber-criminal engaged in such activity: 'crackers', who seek intellectual stimulation from their activity; vandals, seeking revenge; and those who commit fraud, damage computer systems or undertake espionage.[64]

2.96 The recreational hacker or cracker is often out to find bugs or holes in computer security systems and may rearrange or deface web pages. Government sites can be attacked to make a political point, as was the case when US, UK and Australian servers were systematically defaced by 'Pentagard' in January 2001.[65] A small subset of hackers are more malicious and can cause damage through many techniques: denial of service attacks (swamping a commercial web site with so many emails that it cannot cope); computer viruses; the damaging, deleting or erasing of files; and making public confidential information. Still others go on to minor fraud, such as using stolen credit card information to make purchases, or other non-commercial crimes such as cyberstalking or child pornography.

2.97 A number of studies have looked at cyber-intrusion and the perpetrators thereof. A joint 1997 OSCA-Victoria Police survey of computer crime in a representative sample of over 300 Australian companies found that 37% of its sample experienced intrusion or unauthorised use of its computer systems, 90% of which was by insiders.[66] Similar results emerged from a follow-up survey of 350 companies in 1999 by Deloitte Touche Tohmatsu and Victoria Police. One-third of the companies reported an IT attack in the previous 12 months; 83% of intrusions were internal and 58% external; losses exceeding $10,000 occurred in 12% of the attacks; and it was thought that the attacker was most likely to be a disgruntled employee or independent hacker.[67] Of course, internal fraud and retaliatory action of this kind has always been with us - only the methods may now differ. It is usually handled in-house and not often brought to the attention of law enforcement. In the latter survey, for example, 42% of companies attacked did not report the incident outside the company.[68]

2.98 The Australian Computer Emergency Response Team (AusCERT), an operational arm of the University of Queensland and Australia's peak agency assisting in the prevention of computer-based attacks, received 8,197 computer security

---

64 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 23.

65 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 4.

66 OSCA and Victoria Police, *1997 Computer Crime and Security Survey,* pp. 15-17.

67 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 6.

68 ibid.

incident reports in 2000, an alarming increase over the 1,816 of the previous year.[69] The 'incidents' were largely viruses, distributed denial of service attacks or network scans.

2.99 Further evidence of the growth in cyber attacks comes from the annual US Computer Security Institute/FBI Computer Intrusion Squad computer crime and security survey. This survey of information security professionals attracted only 643 responses in 2000 (a 15% response rate) and its results perhaps should not be extrapolated to the cybercommunity as a whole. That said, it disclosed that 70% of respondents experienced unauthorised use of computer systems in 2000; 25% detected system penetration from outside; 27% detected denial of service; 71% detected unauthorised access by insiders; 85% detected viruses; 11% detected financial fraud and 17% detected sabotage of data and/or networks.[70] Financial losses to the 273 respondents who were prepared to report them totalled US$265,589,940.[71] Of the 43% of respondents who conducted electronic commerce on their site, 19% suffered unauthorised access or misuse; 64% reported website vandalism; 60% reported denial of service; 8% reported theft of transaction information; and 3% reported financial fraud.[72]

2.100 One Australian example of the type of computer attack undertaken, and the outcome, is of interest. A 27-year old male known a 'Optik Surfer', who had been working as a computer networking consultant, was refused employment by an ISP. He obtained access to the company's computer network by using the technical director's user account and password, accessed the subscriber database, showed various journalists those subscribers' credit card details, and left a message on the company's home page that its security system had been compromised. The company lost more than $2 million, was required to change its business name and sold off its Internet access business.[73]

2.101 A more recent security breach involved the government's GSTAssist website, when a student, known variously as 'Kelly' or 'K2', was able to access the records of more than 20,000 GST-registered providers and emailed their confidential details to some 17,000 of them.[74]

---

69 ibid., p. 7.

70 Power R., '2000 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues and Trends,* 6(1) Spring 2000, p. 5.

71 ibid., p. 6.

72 ibid., p. 10.

73 Smith, R.G., 'Internet-related fraud: crisis or beat-up?', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 9.

74 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 5.

2.102 How frequently such cases occur is difficult to determine. While there has been considerable media excitement over the hacker phenomenon, the AFP has been involved in relatively few hacking investigations, prompting one Federal Agent to question whether high-volume, low-level hacking attempts were a portent of global catastrophe or merely the high-tech equivalent of someone rattling a locked door.[75]

2.103 Companies have a vested interest in not disclosing that their computer security has been compromised. It may be, as Dr Russell Smith of the AIC has suggested, that the instances of computer fraud are relatively few in comparison with the volume of transactions and that the media, criminal justice personnel, the computer security industry and others all have a vested interest in portraying the problem as more serious than it is.[76]

2.104 The hacking phenomenon is being addressed in the Government's Cybercrime Bill 2001, currently before the Parliament. The Committee recognises its importance in the e-commerce and general crime sphere but will not pursue the topic further as its direct relevance to money laundering is limited.

Regulation of e-commerce

2.105 Since the inception of e-commerce, debate has raged over the level of regulation it requires. In Australia the Information Industries Task Force recommended that what was needed was a non-regulatory, market-oriented approach that would facilitate the emergence of a predictable legal environment to support business and commerce.[77] Given the global nature of e-commerce, what is clear is that Australia must conform with international norms or be left behind.

2.106 In 1996, the United Nations Commission on International Trade Law (UNCITRAL) developed a Model Law on Electronic Commerce, an international legislative template intended to harmonise domestic legal approaches to e-commerce. The Attorney-General set up an Electronic Commerce Expert Group (ECEG) to consider the Model Law's applicability to Australia and any legal impediments to e-commerce here. The ECEG reported in 1998, recommending the enactment of Commonwealth electronic commerce legislation based on the principle of technology neutrality, broad in its operation, and which would remove any legal impediment to a person's use of electronic communications to satisfy legal obligations under Commonwealth law. The recommendations were put into effect via the *Electronic Transactions Act 1999* (Cth) and a national approach encouraged via the development with all States and Territories of a uniform Electronic Transactions Bill.

---

75 Guerts, J., 'fraud@internet.com.au', *Platypus,* March 2000.

76 Smith, R.G., 'Internet-related fraud: crisis or beat-up?', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, pp. 3-4.

77 Information Industries Task Force, *The Global Information Economy: The Way Ahead,* 1997, pp. 71-74.

2.107 The legislation has been described as creating 'a light handed regulatory regime'.[78] Significantly, while it deals with the threshold issue of the legal recognition of electronic signatures, it does not impose a particular authentication framework. The ECEG specifically rejected a public key authentication framework as proposed by Standards Australia and endorsed by the Wallis Inquiry.[79] It did so principally on the grounds of the volatile state of the authentication technology and a desire not to 'pick winners' among, for example, retinal scans, 4-digit PINs and private keys based on assymetric key cryptography. Yet as para. 2.150 details, the Commonwealth Government has proceeded with a voluntary accreditation process in its Gatekeeper Project.

2.108 E-commerce does place a significant amount of personal information in the hands of merchants, information of considerable commercial value. To counter its inappropriate use, the government has amended the Privacy Act to include national privacy principles which will apply to most private sector organisations from 21 December 2001.[80]

2.109 Rather than regulate, the government's approach to e-commerce has been to emphasise consumer education and awareness raising. That such an approach is needed was emphasised by an experiment conducted by ASIC, which set up a spoof millenium bug insurance site that managed to persuade 233 people to be prepared to part with more than $4 million.[81] The kindest interpretation is that the use of technology may give an appearance of legitimacy to what would otherwise be simple fraud.

The money laundering potential of e-commerce

2.110 It is the view of law enforcement agencies both in Australia and overseas that the Internet and e-commerce technology will be primary channels for committing financial crimes.[82] The AFP cited cryptography, the lack of borders and electronic payment systems as the characteristics inherent in e-commerce that will facilitate money laundering.[83] Amongst other reasons for expecting money laundering to increase, the FATF pointed to the growing number of offshore banking and tax minimisation services offered via the Internet; the anonymity provided by Internet banking services; the lack of audit trail through the use of unregulated cyberbanks and credit card processing facilities in tax havens; ready access to counterfeit

78 Attorney-General's portfolio, *Submissions,* p. 217.

79 ECEG, *Electronic Commerce: Building the Legal Framework,* 1998, p. 136.

80 *Privacy Amendment (Private Sector) Act 2000.*

81 Guerts J., 'fraud@internet.com.au', *Platypus,* March 2000.

82 NCA, *NCA & Cybercrime: scoping paper,* June 2000, p. 6.

83 *Submissions,* p. 62.

indentification; access to encryption for secure communications; and an enhanced capacity to move money via smart cards and e-cash.[84]

2.111 While most authorities agree that the e-commerce infrastructure has the potential to assist in the laundering of criminal proceeds, the extent to which it is currently being used to do so is unclear. In the AFP's view, 'e-money laundering is thought to be negligible, for now',[85] and Tasmania Police found it 'not apparent' in that State.[86] While Victoria Police saw that e-cash and e-banking would provide launderers with future opportunities, it has not to date detected significant organised crime usage of computer systems to launder money; rather, the major detected cases related to extortion and the planning of crimes.[87] The NCA also noted that few cases had come to its attention of organised crime groups exploiting e-commerce and Internet banking.[88]

2.112 It may be that law enforcement has failed to detect such activities or, and more probably in the view of the Committee, e-commerce participants or financial institutions have not reported their losses for fear of repercussions in the market place.

2.113 In its scoping paper, the NCA outlined a case which did come to light. Two 18 year old boys in the Welsh town of Dyfed-Powys were charged with breaking into electronic commerce Internet sites in five countries and stealing information on 26,000 credit card accounts. The investigation involved the United States Federal Bureau of Investigation, the Dyfed-Powys Police Service and the Royal Canadian Mounted Police. According to an FBI spokesperson, the boys were alleged to have hacked into nine e-commerce web sites in the United States, Canada, Thailand, Japan and the United Kingdom; losses were estimated at approximately US$3 million.[89]

2.114 To what extent *organised crime* is exploiting the potential of e-commerce for *money laundering,* as opposed to individuals exploiting the potential of e-commerce for individual gain, or revenge, or amusement, is even more difficult to ascertain.

2.115 When money laundering techniques are considered in parallel with e-commerce realities, a number of possible challenges become clear. The use of cryptography has an equal potential to assist criminal communications as it has to secure legitimate transactions. While new technology can be employed to good effect to assist in the tracing of communications, electronic evidence is relatively easy to destroy. E-commerce has a global reach and individual jurisdictional laws could be exploited by money launderers living in one jurisdiction, perpetrating offences in a

---

84 FATF, *Report on Money Laundering Typologies 1999-2000,* OECD, Paris, 2000.

85 *Submissions,* p. 63.

86 *Submissions,* p. 43.

87 *Submissions,* p. 55.

88 *Submissions,* p. 162.

89 NCA, *The NCA and Cybercrime: Scoping Paper, June 2000,* p. 27.

second jurisdiction and transferring value through many other jurisdictions. And although it is perhaps too soon to tell which of the new electronic payment systems will become most widely used, and which user identification techniques will develop, they all present some possibility of exploitation by criminal elements for money laundering and other purposes.

2.116 Of particular concern is the potential of the stored value card to assist in money laundering. If stored value technology becomes widely accepted, it will present a considerable threat, particularly if the value stored is high. In a way not dissimilar to high-value banknotes today, highly portable stored value cards could facilitate money laundering. Some stored value systems have detailed audit trails because fund transfers are effected through regulated financial institutions; others, such as the UK Mondex system, might have only limited audit trails.[90] If e-commerce begins to operate outside of the regulated financial system, transactions are essentially untraceable. Alternative forms of digital cash may cause similar concerns.

Next steps

2.117 Policing of cyberspace raises some interesting challenges for the global community, not only for law enforcement. The approach to crime control will be, perhaps more than ever, a shared responsibility among law enforcement agencies, the e-commerce and IT industries themselves and the individual user. The view put forcefully to the Committee by representatives of the Attorney-General's Department was that 'the first line of defence should be self-defence';[91] that effective protection from threats within the electronic environment will require risk management strategies by the private sector and private individuals, albeit with government and law enforcement agency encouragement and assistance.[92]

2.118 However, having taken a positive role in promoting e-commerce, the government clearly has a duty to ensure that the public can engage in e-commerce safely and with confidence that, in the event of major mishap or misuse, law enforcement agencies are able to step in. Various provisions to achieve this were advanced during the Committee's inquiry. The AGEC Action Plan, which was warmly supported by the NCA, called for the following key issues to be addressed:

- develop joint public and private sector strategies to raise awareness and manage risks associated with the information economy;
- improve IT skills in the public and private sectors;
- develop appropriate interception, computer forensics capabilities;
- advocate appropriate levels of electronic authentication;

---

90 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 105.

91 *Evidence,* p. 29.

92 *Evidence,* p. 26.

- facilitate appropriate record-keeping standards for ISPs; and,
- effective administration of mutual assistance and extradition arrangements.[93]

These are all sensible suggestions. The Committee has considered interception capabilities and the possible regulation of ISPs in Chapter 1; it addresses mutual assistance and extradition matters in Chapter 3. In the remainder of this Chapter it considers in particular the matters of awareness-raising, public-private sector partnerships, electronic authentication, and whether a computer forensics capability is required. It also looks briefly at whether there is a role for government in regulating access to electronic tools of crime such as strong cryptography.

Awareness-raising

2.119 Several witnesses took the view that, to a considerable extent, responsibility for preventing e-crime lies with e-commerce participants themselves. Just as car theft is discouraged by the owner taking precautions such as locking doors and fitting immobilisers, so e-commerce participants should engage in target-hardening practices.

2.120 From the business point of view, these could include appropriate levels of IT security, a preparedness to verify customer identity and to deal only with properly authenticated businesses, all of which would have the added benefit of reducing any money laundering potential of e-commerce.

2.121 From the point of view of the individual customer, again the question of appropriate IT security applies, but equally it is a case of *caveat emptor,* or buyer beware. Customers should be prepared to check on the credentials of Internet companies before they entrust them with their orders and credit card details, just as they do when choosing to buy through mail order.

2.122 The Police Commissioners' Conference Electronic Crime Strategy recognises a role for police in awareness-raising. One of its objectives is to 'create a safer community by contributing to community education about electronic crime, cyber ethics and how best to avoid victimisation';[94] key activities are to produce and deliver crime prevention information detailing how to avoid or minimise victimisation and to support private organisations in the production of consistent and useful consumer protection information.

2.123 Other government agencies have already taken practical steps to bring these matters to general attention. NOIE, through its 'Shopping Online?' project, has produced a useful series of consumer awareness publications on the risks and benefits of online shopping.[95] To overcome the problem of cross-border Internet fraud, a

93 *Submissions,* p. 147.

94 ACPR, *Electronic Crime Strategy of the Police Commissioners' Conference Electronic Crime Steering Committee 2001-2003,* 2001, p. 15.

95 www.noie.gov.au/projects/consumer/shopping_online/index.htm

multilingual website www.econsumer.gov is proposed, to provide information on consumer protection laws in 13 countries and offer consumers a way to file complaints online. The cooperating governments will use a parallel, but secure, site to share complaint data and information on e-commerce fraud investigations. Australia's participation is through the ACCC.[96]

Public-private sector partnerships

2.124 New technologies may provide the means by which e-crimes such as fraud and money laundering are facilitated, but they can also be expected to furnish the means by which such crimes will be able to be detected. AUSTRAC's use of artificial intelligence to pinpoint suspect transactions below the reporting threshold is a case in point.

2.125 It is generally accepted that the newest technology and the greatest IT expertise resides in the private sector, for the simple reason that the private sector has most to gain from its commercial exploitation and has fewer constraints in paying for it. As Mr Murray Rankin, of the private sector firm, The Distillery, told the Committee:

> a lot of the potential [public sector] users of private sector products take the decision to use what would arguably be inferior products because of things such as budget constraints ... They are prepared to accept a lesser service at a cheaper cost ...[97]

2.126 Criminals are using advanced technologies to commit crimes, as the ABCI illustrated with the case of the 'Post-card Bandit', Brendan Abbott, who was in possession of a small arsenal of technological aids when apprehended.[98] Law enforcement has always faced an enormous challenge in terms of keeping up with the technology available to the better-resourced criminals. Given the specialist nature of some of the latest technology, and its relentless and rapid advance, the only real option for government in general, and law enforcement in particular, is to enter into increasing partnership with the private sector in terms of both technology and expertise.

2.127 There appears to be little consensus, however, on the format such public-private sector 'partnerships' might take. At one end of the spectrum, there are jointly funded and operated cybercrime agencies; at the other, there is the employment of private sector experts in public agencies on contract. In the middle, there are 'partnerships' in the sense of joint working parties and consultative forums.

---

96 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 14.

97 *Evidence,* p. 83.

98 *Submission,* p. 128.

2.128 Some commentators envisage for Australia a structured model based on the National Infrastructure Protection Center's Infragard in the USA, whose secure website provides members with information about cyberintrusions and appropriate protections; or the Internet Fraud Complaint Center, a joint initiative of the FBI and the National White Collar Crime Center, to which crimes can be reported via a secure web page for investigation and referral to the appropriate law enforcement body. More integrated public-private cooperative ventures are being developed in the United States, including the recent formation of an IT Information Sharing and Analysis Centre. Government agencies and 19 technology vendors, including Cisco Systems, IBM, Hewlett-Packard and Microsoft, are said to have formed an alliance in order to set up a secure mechanism that they can use to exchange information about security vulnerabilites such as viruses and other potential threats to corporate and govenment computer networks.[99]

2.129 'Partnerships' involving the employment on contract of private sector experts by public sector agencies have in fact been underway for some time. Mr Gordon Williamson, Director of AFP Technical Operations, told the Committee that when a very high level of technical expertise was required, the AFP contracted it in from those at the cutting edge, as no agency could justify having it 'on tap' the whole time. He assured the Committee that the AFP had not been in the position of being unable to resolve an investigation because it lacked the necessary expertise:

> All the way along we have either had internally, or through relationships with our partner agencies *or other private industry sectors,* the right level of expertise to bring to bear on the job at the time.[100] [emphasis added]

2.130 The Committee was told of similar practices in a number of agencies. ASIC outsourced its computer forensic requirements to the AFP or to the large accounting firms.[101] AUSTRAC director Elizabeth Montano indicated that her agency also contracted in the computing expertise her agency needed, with contractors being paid market rates; however the agency also maintained sufficient in-house expertise to ensure that it was not being 'conned'.[102] CrimTrac representative Mr Kim Terrell described the IT industry as being very open and flexible in terms of the relationships it would enter into with the public sector and his aim for CrimTrac would be one of strategic partnerships with industry.[103]

2.131 While contracting in IT expertise was the pragmatic choice of many law enforcement agencies, it nevertheless raises security concerns. Mr Geoff Gray of the Commonwealth DPP's Office voiced the concerns of many when he stated:

---

99 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 12.

100 *Evidence,* p. 146.

101 *Evidence,* p. 160.

102 ibid., p. 43.

103 ibid.

> there are great limits to the extent to which you can bring in those private sector skills. From my point of view, I would much prefer to see [computer forensic skills] remain within the AFP. People speak in glowing terms about contracts, but I just do not see how you can prevent leakage of confidential information. It is very much a second-best option, in my opinion.[104]

2.132 An even more fundamental question is whether there are sufficient suitably qualified people in either the public or private sectors to meet law enforcement's IT needs. Mr Rob Durie, Executive Director of the Australian Information Industry Association, told the Committee that there was an overall shortage of about 30,000 persons in the general IT field, let alone in highly specialised areas, and that present initiatives to provide extra places at universities were impeded by the lack of teachers and in any event would show no results for five years or more.[105] He reinforced the view that government-industry partnerships were the only realistic option.

2.133 The Committee received a great deal of evidence of the existence of a number of consultative forums and working groups, including the Law Enforcement Advisory Council (LEAC), the newly formed law enforcement taskforce chaired by the IIA[106] and the National Information Infrastructure Consultative Industry Forum.[107]

2.134 The e-crime strategy from the Police Commissioners' Conference particularly stresses the need for a cooperative relationship between law enforcement, the industries providing the networking and IT services, and the industries actually using the services.[108]

2.135 In relation specifically to e-commerce, AFP Commissioner Mick Keelty stressed the two-way nature of private sector partnerships with law enforcement. He noted that the private sector was producing or using technology for commercial reasons and hence it should be prepared to invest in its protection. He indicated that the general run of calls for assistance that the AFP received were largely from businesses complaining that their website had been hacked into, because they had inadequate or no security in place. He noted that the private sector response to proposed police-initiated security information forums had been 'pitiful'.[109]

2.136 Specific-issue working partnerships to deal with matters such as identity fraud appear to have been more successful. The NCA's Swordfish Task Force has established a Joint Agency Forum in NSW which has recognised the need, inter alia, to work with the private sector to encourage and assist in developing identity-checking

---

104 ibid.

105 ibid., pp. 69-70.

106 AGEC, *Submissions,* p. 253.

107 AIIA, *Evidence,* p. 77.

108 Police Commissioners' Conference, *Electronic Crime Strategy,* March 2001.

109 *Evidence,* p. 148.

strategies and to progress MOUs between law enforcement and regulatory agencies with respect to sharing identity data.[110]

2.137 The Committee notes that there is no one strategic relationship for all occasions, but those strategies which involve some form of public-private partnership will almost certainly be more effective. This partnership issue arises directly in the next section: in relation to the establishment of a national cyber-forensic unit.

A national cyber-forensics unit?

2.138 The capacity of law enforcement to keep up to speed with technological change was a recurring theme in evidence to the Committee. The RGEC report addressed the question of law enforcement's future computer forensic skills requirements and concluded:

> Many of the countermeasures to crime which exploits the characteristics of the Internet call for law enforcement and revenue agencies to use sophisticated tracing and other tools. They also call for these tools to be used by well trained specialists who retain their skills and maintain contact with industry. This would be a significant ongoing expense for government. To ensure such an investment is used effectively and as widely as is needed Australian governments should address the provision of a central computer and Internet forensic capability, available to all Commonwealth, State and Territory jurisdictions to support the investigation of computer and Internet-related crime.[111]

2.139 The Committee learnt that the AFP has electronic evidence teams of 12 and was 'upskilling' all its officers to a basic level of computing competence. AFP Commissioner Mick Keelty assured the Committee that 'at the moment we are meeting demand'[112] The NCA was doing much the same, maintaining an in-house capability for straightforward retrieval of electronically stored data,[113] but the question remains whether present approaches will suffice in the potentially more challenging technological future.

2.140 The NCA was firm in its view of the need for the establishment of a national law enforcement cyber-forensics facility for highly sophisticated data recovery. It acknowledged, however, that it was not practical or cost-effective for an organisation of the NCA's size to seek to develop such a capacity in-house. It would prefer to rely

---

110 *Submissions,* p.166.

111 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1, 1999, p. 119.

112 *Evidence,* p. 155.

113 NCA, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the management arrangements and adequacy of funding of the Australian Federal Police and the National Crime Authority,* February 2001, p. 23.

on a common national resource to provide the service.[114] The ABCI stressed that such a facility need not be a bricks and mortar establishment but that there was merit in considering a virtual capacity that used the specialist expertise in a number of organisations.[115]

2.141 The AFP confirmed the RGEC view that no agency could justify having on tap very high level technical expertise in every field. Faced with a request to investigate a high level attack on a banking system, the AFP now would contract in the expertise of those at the cutting edge.[116] As Mr Williamson explained, to maintain expertise you need continued work in a specific area, and the people who have that continued work are in the workplace or research centres. They are the people the AFP would seek to co-opt or contract as the need arose.[117] He added that the AFP would seek to maintain cutting edge expertise in-house in specific areas such as cryptography, which is always required.

2.142 The Committee notes that in the defence and security fields in Australia, the need for high-level computer capabilities has been recognised and acted upon. Following the Dudgeon and Cobb reports of 1997, a National Information Infrastructure Protection Secretariat was set up, and the National Computer Authority within the Defence Signals Directorate was expanded, as was the Defence Science and Technology Organisation's Advanced Computer Capabilities Branch. The latter was reported as employing over 40 scientists and professional software and hardware engineers in April 2000.[118] The computing needs of the law enforcement community should be reviewed in this context.

2.143 In the law enforcement field overseas, specialist cyber-forensic facilities have already been set up. In the USA, the National Infrastructure Protection Center was established in 1998 at the FBI; the DEA also has a Computer Forensics Program, now located in the Office of Forensic Sciences. The number of cases handled by the latter is reported as increasing at a rate of 30 per cent per year.[119]

2.144 In the Committee's view, the case for a cyber-forensic facility in Australian law enforcement seems persuasive. While a modest level of technological knowledge of data recovery or interception can be expected of law enforcement officers in all agencies, it would not be cost-effective, practical or even possible for all agencies to develop sophisticated in-house cyber-forensic capabilities. A shared facility is clearly the only realistic option. And while the Committee accepts the need for a close

---

114 NCA, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the management arrangements and adequacy of funding of the Australian Federal Police and the National Crime Authority,* February 2001, p. 23.

115 *Evidence,* p. 102.

116 *Evidence,* p. 147.

117 *Evidence,* p. 153.

118 NCA, *The NCA and Cybercrime: scoping paper,* June 2000, p. 29.

119 ibid., p. 32.

relationship with private sector expertise in this area, it believes there is a legitimate and very necessary role for a government facility to play.

2.145 The Committee therefore recommends that a national cyber-forensic facility be established. The Committee expresses no firm view on the location, size, precise format or funding arrangements for such a facility but notes that there are common police services which might serve as a model. In the planning of a cyber-forensic facility, particular attention will need to be paid to issues of recruitment and retention of relevant expertise.

Recommendation 9: That a national cyber-forensic facility be established.

2.146 In the longer term, a more ambitious broadly based cybercrime unit might be considered in Australia. Both the UK and the USA have moved in this direction. In the UK, the National Criminal Intelligence Service (NCIS), in its study of computer crime, recommended that the most successful method of policing serious computer misuse was via a single, dedicated national unit. Its role would be to investigate the more serious IT crimes, to act as a centre of excellence for cybercrime issues and to support local police forces in their investigations.[120] The recommendation was accepted, and it has been announced that some £50 million has been provided to build a national computer crime unit.[121]

2.147 Of the many developments in the cybercrime prevention field in the United States, one of the more interesting from the perspective of Australia has been the establishment by the FBI of a centralised capability for cybercrime investigations. The National Infrastructure Protection Center (NIPC) at FBI headquarters is overall program manager; 16 FBI field offices will have NIPC squads of seven or eight agents each, with nationwide, 193 agents dedicated to investigating NIPC matters.

2.148 It was recognised at the time of formation of the NIPC in 1998 that it could not accomplish its mission to 'detect, deter, assess, warn of, respond to, and investigate intrusions and illegal acts that target or involve [US] critical infrastructures' without outside assistance. Hence the setting up of the NIPC Outreach strategic partnership program, involving all levels of government and various private sector organisations. A secure communications network, InfraGard, connects the partners. Other initiatives include the National Cybercrime Training Partnership, and the Computer Analysis Response Team, with 142 personnel specialising in the recovery of evidence from electronic media. The FBI has been reported as anticipating

120 NCIS, Project Trawler:Crime on the Information Highways, NCIS, London, 1999, p. 23, as cited in Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 72.

121 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 72.

that, with the likely increase in high-tech crime, the number of required computer forensic examinations will rise to 6000 this year.[122]

Electronic authentication

2.149 It is widely accepted that the success of e-commerce depends on a trusted, open authentication framework since, without authentication, nobody can be sure of who or what they are dealing with over the networks. Authentication in the context of e-commerce is the means of proving who you are.

2.150 For commercial purposes, more complete authentication associating an individual's public key with other identification characteristics has been sought and possibly found in the form of digital certificates, issued by a trusted third party to identify the certificate holder. There has been a growth industry, particularly in the United States, in companies setting up as issuers of digital certificates. In Australia, the Commonwealth Government saw the need for a strategy to control the issue and management of digital certificates, for the secure delivery of Government services online as well as to encourage the uptake of e-commerce in the private sector. In October 1997 the then Office of Government Information Technology established Project Gatekeeper to develop a national framework for the authentication of users of electronic online services, consistent with the OECD Guidelines on Cryptography Policy. To date, the Australian Taxation Office, Baltimore Certificates Australia Pty Ltd and Health eSignature Authority have achieved full Gatekeeper accreditation; eSign Australia Ltd has achieved entry level accreditation and 17 other organisations are seeking accreditation to issue Australian Business Number Digital Signature Certificates (ABN-DSC).[123]

2.151 The private sector has been active in this area, with Australia's four major banks collaborating on Project Angus to issue digital certificates later this year to business customers; those certificates will exist in the global Identrus electronic trust and payments scheme but will also be recognised as ABN-DSC digital certificates and will be accepted by Commonwealth agencies.

2.152 To ensure national uniformity in this regard, the States and Territories agreed in November 2000 to the Gatekeeper strategy and to adopt the ABN-DSC initiative. A Gatekeeper Policy Advisory Committee has also been established. The end result should be that government agencies will be able to chose from a panel of service providers whose products and methods of delivery have been evaluated and accredited to meet appropriate standards of integrity and trust.

---

122 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, pp. 78-81.

123 www.govonline.gov.au/publickey/abn-dsc-angus.htm, visited 16 July 2001.

Regulation of high-tech tools?

2.153 Law enforcement agencies and others have occasionally voiced the opinion that the way to prevent misuse of advanced technological tools is to place restrictions on their sale to the public. In particular, software permitting the generation of false credit card numbers, or software providing high-level encryption, have been suggested as candidates for such treatment. Until quite recently, strong cryptography was the monopoly of defence establishments, yet now it has been democratised to the point that anyone can download it free from the web, although the Committee was told that the export of certain cryptographic products was still banned in the United States.[124]

2.154 Not surprisingly, industry groups were in favour of the free flowering of new technology, unimpeded by government intervention. The Australian Information Industry Association, for example, told the Committee:

> Industry should be permitted to develop, invest, innovate and market new products and services, the viability of which will be determined by market demand. New technology offences cannot be addressed by restricting access to the *technology*. Rather, it is the *use* to which they may be put that may lead to an offence being committed. Where necessary, potentially "dangerous" products, such as high level encryption, should be licenced rather than banned.[125]

2.155 In evidence to the Committee, Mr Marshall Irwin, Member of the NCA, suggested that 'trying to stop encryption is probably like King Canute trying to hold the tide back'[126] and that what law enforcement needed was the ability, in appropriate circumstances, to be able to go behind the encryption and to intercept and decode email messages.

2.156 Despite a superficial attraction to regulating access to technological tools which have a capacity to thwart law enforcement, the Committee recognises that, if it exists, the Brendan Abbotts of the criminal fraternity will gain access. Law enforcement simply has to find other ways to handle the situation.

Conclusions

2.157 Through its willingness to adopt new technology, Australia is well positioned to benefit from e-commerce. While certain characteristics of e-commerce, such as its global spread, its accessibility, its immediacy and use of cryptography, lend themselves to potential exploitation by money launderers, there is little evidence to date that it is being so exploited. A long list of traditional offences, including identity theft and fraud, have been facilitated by advances in mobile telephony, the Internet

---

124 *Evidence,* p. 65.

125 *Submissions,* p. 73.

126 *Evidence,* p. 21.

and encryption; and it is these developments, more than e-commerce per se, that have the potential to assist money launderers.

2.158 It seems to the Committee that lax security of computer systems and human negligence (or lack of integrity) are the chief culprits in much e-crime. The answer lies, not so much in law enforcement, but in target hardening. The technology is there, and is improving all the time and decreasing in cost, to thwart illegal access and to some extent at least to lessen the chances of system compromises from within.

2.159 From the evidence provided to it, the Committee believes that the NCA and its partner agencies are well aware of the potential law enforcement risks posed by e-commerce and are developing strategies or have strategies already in place to counter them. It is now a question of continuous monitoring of new technological and payment developments, and of continuous reassessment of law enforcement responses, supplemented by upgrading of officers' skills and by the establishment of a specialist cyber-forensic facility.

2.160 To meet the jurisdictional challenges of both e-commerce and money laundering, continued international negotiations are required to harmonise definitions of e-crime and search and seizure provisions, to synchronise law enforcement mechanisms and to extend and improve extradition and mutual assistance treaties. These matters are addressed in the following Chapter.