Chapter 4

Banking, Credit Card Fraud and Money Laundering

The banking industry

4.1 Most Australian consumers are affected in one way or another by electronic banking. The banks use their cyberspace networks to process transactions, and to communicate with the many clients who have taken up Internet banking. The potential for cyberfraud covers a number of banking areas. They include Internet banking, credit and debit card fraud, money laundering and related offences such as identity theft and securities and investment fraud.

4.2 The Australian Bankers' Association (the ABksA) appeared before the Inquiry and also provided a submission. In the introduction to its submission the ABksA indicated its position on the subject of the Inquiry:[1]

- The current regulatory framework covering cybercrime is satisfactory and no further legislation or regulation is required at the Commonwealth level.
- Customers have a vital role to play in protecting their own interests, and banks will continue to provide financial literacy programs including cybercrime self-protection.
- State and Federal Governments also have a vital role to play in providing education programs to ensure customers better understand their responsibilities in protecting their own interests.
- The banking industry is a vital component of the critical infrastructure that underpins the whole of the Australian economy and Government should assist banks and other stakeholders in protecting this national asset.

4.3 The Committee notes the banks' emphasis on consumer responsibility for self protection from fraud, rather than the banks' duty to protect their customers. This emerged as a significant issue during the course of the Inquiry. The Committee notes that both consumers and banks have a number of options at their disposal to increase fraud protection. This chapter notes the most significant of those options.

Internet banking

4.4 Internet banking allows bank customers to view statements online, pay bills, transfer funds between accounts, make inquiries, order cheque books, and to do almost anything which can be done at the bank itself, except withdraw cash!

---

1 Australian Bankers' Association, Submission no.19, p.5

4.5 Internet banking is subject to all the same financial transaction reporting, proceeds of crime and taxation laws as other banking services.[2]

4.6 Banks have been enthusiastic in their encouragement of clients to adopt Internet banking as noted in the ABksA submission:

> Banks have embarked on the development and deployment of Internet banking facilities because the market has demanded that banks provide a secure and trusted environment for the delivery of a wide range of financial services in a convenient and cost effective manner. [3]

4.7 The development of e-banking, and its acceptance by society has seen the emergence of new ways to perpetrate 'old' crimes such as fraud and money laundering and the development of new crimes. These crimes are using and at times taking advantage of the same technology as e-banking.

4.8 The evidence presented to the Committee revealed different ways of manipulating the Internet banking environment. Apart from the Nigerian email letters in which criminals set up false 'authentic' accounts to receive the transferred money, there have been bogus bank sites established which then request 'confirmation' of account details – such as passwords and account numbers. The Committee heard that it is not difficult to duplicate features such as the logo of the bank, and the layout of the website, all of which is designed to deceive the bank customer.[4]

4.9 In evidence, the Australian Bankers' Association noted that the banks in the bogus bank example were able to respond with the assistance of the Australian Federal Police[5] within hours and the sites were shut down. The banks also emphasised in the ensuing publicity that banks never request 'verification' of details through the Internet, and that passwords should be revealed to no-one.

4.10 The Committee notes the comments of ASIC who acknowledged the role of Internet technologies in providing new opportunities for people to engage in new types of scams such as the email referred to above. ASIC said in evidence:

> … Without spam and Internet technology, that crime would not occur. The fact that we have seen reported in the press something like half a dozen of those matters in the last three or four months does not necessarily equate to a flood. To balance that up, … they very quickly were able to identify the Australian connection, they worked with the New South Wales Police, and someone was arrested within three days of that spam email going out. I understand that person has been charged subsequently with deception. … it

2 Submission no. 23, p. 23

3 Submission no. 19, p.19

4 *Committee Hansard*, 18 July 2003, p. 44

5 *Committee Hansard*, 18 July 2003, p. 44

> appears that the financial institutions, working with the police services, are able to protect themselves adequately and take recourse.[6]

Prevention – Internet banking security

4.11 The Committee notes that the ABksA indicates that banks are addressing prevention and detection of criminal activity in banking and credit card transactions through a number of avenues. [7]

4.12 In relation to the issue of prevention, the Committee received evidence which revealed some concerns regarding the security of Internet banking. A submission from Mr Tony Healy[8] expressed concern that banks do not use strategies which can assist with the prevention of Internet banking fraud.

4.13 Mr Healy notes that traditionally, retrieval of funds from an account required the presentation of a physical token (passbook or ATM card) combined with secret information (PIN or personal signature).

4.14 When Internet banking commenced, the second element was provided through digital certificates, given to each client and installed on the client's computer. However, these were expensive, and banks moved to the cheaper option of password protection only. Mr Healy considers this is weak protection, as passwords can be obtained through the activity of viruses or through being stored on the browser, and thus being available to any user of that computer.

4.15 Finally, Mr Healy notes that the customer is responsible for the security of the password, and under most electronic banking contracts, its revelation even if not by the client, constitutes negligence.

4.16 Mr Healy was not alone in his disquiet. In evidence to the Committee Mr Steve Orlowski said that in the current banking environment the standard of Internet banking security is 'just' adequate,[9] and most of the problems occurring at the moment are due to inadequacy of the banks' protective anti-hijacking measures. Mr Orlowski continued:

> The Internet itself is not the problem; it is what is happening at the end point where the data is being held.[10]

4.17 The Committee was concerned, that despite the banks' confidence in their security, there are clearly significant data protection issues which concern the experts

---

6 *Committee Hansard,* 21 July 2003 p. 47

7 Submission No. 19, pp. 13-14

8 Submission no. 14, p. 2

9 *Committee Hansard*, 17 July 2003, p. 7. Mr Orlowski is a private consultant and is also the chair of APEC's eSecurity Task Group.

10 *Committee Hansard*, 17 July 2003, ibid.

in the area. Mr Orlowski noted that the banks are moving towards stronger protection and will be implementing an electronic authentication system. This is expected to provide a much stronger access control technique for users.

4.18 The Committee considers that part of the solution is to use public education campaigns to prevent customers from being defrauded by fictitious websites. However the Committee does not accept the assertion of the banks that this is solely the role of government; it is clearly part of the banks' client service role, to provide information to its customers, which as far as possible ensures that they deal with the bank itself.

4.19 In evidence ASIC noted that its interest is very much from the consumer protection angle. ASIC ensures that financial institutions are aware of the threats, that they implement appropriate risk management strategies, provide clear instructions to their clients about their obligations and liabilities, as well as educating them about safe practices.

> Having said that, there is no doubt that the arrival of the Internet technologies of the Internet technologies has provided new opportunities for people to commit new types of scams … [In] one of those matters involving a large Australian financial institution … they very quickly were able to identify the Australian connection, … and someone was arrested within three days of that spam email going out.[11]

4.20 While noting ASIC's comment and the fact that there was a rapid response to the attempted fraud, it is only a matter of time before other ways of breaking into banking records are devised. In the Committee's view there is no room for complacency. The Australian Crime Commission (ACC) in conjunction with the Australian High Tech Crime Centre (AHTCC) are in a position through their intelligence activities to provide general information about fraud trends to financial institutions. This information could be provided through a third party which could collect and disseminate all available information on a regular basis.

Recommendation 5

The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.

Credit and debit card fraud

4.21 The introduction of the Bankcard to Australia by nine Australian banks in 1974, commenced a revolution in consumer purchasing. While some stores had offered credit cards and store based finance for many years, the concept of a

11 *Committee Hansard,* 21 July 2003, p. 48

universal credit card administered by the banks allowed bank-funded credit to be extended to new areas of consumer activity.

4.22 With the credit card purchasing power came the potential for large scale fraud. Advancing technology changed only the method of committing the fraud and has also required technological expertise used to investigate and detect fraud to advance.

4.23 Card Skimming involves a small device which will capture the card details for use in a reproduced card. In its submission to the Committee, the ACC noted that it is not only credit cards which can be skimmed for their information. These devices are also used at Automatic Teller Machines (ATMs) and card skimming can be used to obtain personal information from debit cards, and even Medicare cards. Over the past 12 months, credit card skimming alone has increased bank losses by 400 percent, and its actual cost to the banking industry, businesses and consumers is more than $300 million per year.[12]

4.24 In evidence, the NSW Police advised that a Fraud Squad task force had found that one of the main areas of card fraud is 'points of common purchase'.[13]

> A common purchase point is an area, usually a service station, where someone skims a user's card. The information is then passed on to criminal syndicates who reproduce cards en masse and on-sell them again … Service stations are about 75 per cent of the common purchase points.

4.25 The Committee was also informed in the ACC submission that card skimming is being perpetrated by organised crime groups:

> in conjunction with other serious cross jurisdictional and transnational criminal activities including drug trafficking, money laundering and potentially arms trafficking.[14]

4.26 The ACC also notes 'the social implications of card skimming are serious'.[15] Apart from the cost to banks, the victims are left with debts in their name for which they are held responsible unless and until the victim can show otherwise. The Commission continued:

> the rising incidence of credit card skimming is leading to the introduction of new controls that would shift the onus of harm from the financial sector to individuals. Such countermeasures are likely to impact adversely upon individuals.

---

12 Submission no. 23, p. 25

13 *Committee Hansard,* 18 July 2003, p. 87

14 Submission no. 23, p.30

15 Submission no. 23, p 27

4.27 The Committee shares the concerns of the ACC. The social and financial cost of forcing consumers to pay for harm resulting from credit card fraud is potentially high.

Merchants and credit cards

4.28 The Committee also heard from Mr Graeme Bond, a merchant who has had an ongoing disagreement with his bank since 1996, regarding a series of fraudulent credit transactions for which the bank has held him responsible. The Committee notes that Mr Bond's experience is more about a fraud which was perpetrated by means of a credit card, and the arrangements with his bank, than an Internet transaction. Mr Bond's experience illustrates the nature of the liability imposed through the agreements between banks and merchants.[16]

Prevention – Credit Card Skimming and Fraud

4.29 The ACC advised the Committee that credit card skimming has been approved by the ACC's Board as an approved intelligence investigation. Thus far, the activity has consisted of consultation with:

- New South Wales Police about their Task Force Venlo, which investigated credit card skimming in New South Wales;
- Discussing with the (credit) card companies risks and trends and what they believe law enforcement should be looking at in relation to card skimming.
- Participation in the MasterCard fraud reduction task force meeting.[17]

4.30 The ACC also noted that the card skimming appeared to have 'migrated' from South East Asia. The Committee observed that as the reference is quite recent, the ACC is still in the early stages of developing strategies. The ACC did advise the Committee that the AFP liaison network was doing some work in this area.[18]

4.31 The Committee was also told of a system of random checks to validate credit transactions which the banks undertake each day. In particular, if there are any unusual features of a transaction, the card holder will be contacted to check it was made by the card owner. The Committee was told that there are over 300 such calls made each day, and that the banks wear significant losses for the transactions fraudulently made.[19]

4.32 The Attorney General's Department pointed out that a number of peak bodies are developing ways in which card skimming can be eliminated. These include the Standing Committee of Attorneys General, the Australian Police

16 Submission No. 16

17 *Committee Hansard* , 18 July 2003, p.11

18 *Committee Hansard* , 18 July 2003, p.11

19 *Committee Hansard* , 18 July 2003, p.11

Ministers' Council, the Australian Bankers' Association, and a Commonwealth NSW task force.

4.33 However the banks do have other technology available. The so-called 'smart card' is a far more secure option than the magnetic stripe technology in current use.

> A smart card is made of plastic, and in size and appearance is similar to a normal credit card. [The card has a] microchip embedded in it … which replaces the magnetic stripe commonly found on the back of other transaction cards. [It] allows the storage and management of large amounts of different types of information. Most importantly, the microchip may allow the performance of computing tasks through a microprocessor included in the chip. Using the integrated circuit's memory capacity and processing power, one card can accommodate multiple applications providing greater flexibility and ease of use for the customer.[20]

4.34 The technology is used in security applications, and is difficult to replicate. It is expensive to produce, but is far more secure than its alternatives, and may represent a saving for financial institutions in the long term.

4.35 The Committee observes that banks and the promoters of credit cards derive considerable income benefits from their use by consumers and merchants; the cards are strongly promoted in many contexts. An example is the special sporting events cards, promoted and used initially at times when there are many itinerant people in one place, who are being encouraged to spend. The potential for fraudulent use in such circumstances represents an increased risk. Where the card holder can be shown to have been reckless in the care and storage of the card and its details, it is clear where the liability for misuse lies. In cases where neither the financial institution nor the cardholder has compromised security, there is clearly an increased cost to the bank which should not be borne entirely by either the bank or the client cardholder.

4.36 However, in cases where neither the financial institution nor the card holder has been negligent, the allocation of liability is not nearly so clear. The approaches currently available to resolve this issue were developed in pre-electronic banking, pre-Internet times. The Committee is of the view that given the increased potential for fraudulent use in the e-environment, the issue warrants an approach which is grounded in the electronic transmission of documents, rather than their physical presentation.

Identity fraud

4.37 Closely associated with banking and credit card fraud is identity fraud. The Victoria Police told the Committee hearing that identity related crimes are evident in most fraud related offences, including loan applications, credit card fraud and online

20 http://www.smartcardforum.asn.au/smartcard.htm

banking. Globally, this activity is currently one of law enforcement's greatest problems.[21]

4.38 The ACC noted in its evidence that identity fraud is used as a means to commit drug, firearms and e-crime offences.[22] Identity fraud offers opportunists and those who shift from one area to another an easy way to pursue the quickest way of making money, whether it is by drugs, guns, prostitution or white-collar crime.

4.39 In this context, one of the issues which arose was the integrity of the 100 point check, used by banks to establish the identity of a person wishing to open an account. The system is established under the *Financial Transaction Reports Act 1988*. As AUSTRAC pointed out in evidence, the documentation was not created with the identification system in mind:

> Birth certificates, passports, drivers' licences and even credit cards – all these sorts of things – can be used as part of the process. The system is okay; it is the integrity of the documents and the ability to verify them that creates the difficulty in the process.[23]

4.40 The ABksA advised the Committee that new technologies such as scanners, and colour printers have increased the banks' exposure to identity fraud, and that it is relatively easy to produce false documents of high quality.[24]

4.41 The Committee notes that while the 100 point check in itself is clearly a useful tool – 'a robust identification system' – the issue is increasingly the underlying integrity of the documents.[25]

4.42 In evidence, AUSTRAC told the Inquiry of a Proof of Identity Committee chaired by AUSTRAC which is examining some of the options which might be available to verify claims to identity.[26] AUSTRAC suggested that a system of fast-track verification of documents would be of benefit and also suggested the possibility of a facial and iris recognition system known as biometrics.

4.43 This was also raised by Standards Australia which has developed a number of standards for the use of information technology in the banking system, for example, the maintenance of security for the operation of ATMs.[27]

---

21 *Committee Hansard*, 17 July 2003, p. 37

22 *Committee Hansard*, 18 July 2003, p. 11

23 *Committee Hansard*, 18 July 2003, p. 64

24 *Committee Hansard*, 18 July 2003, p. 45

25 *Committee Hansard,* 18 July 2003, p. 64

26 *Committee Hansard*, 18 July 2003, p. 63

27 *Committee Hansard*, 18 July 2003, p. 52

4.44 Biometrics is the identification of people through face recognition, fingerprints, iris recognition, retina recognition (visual recognition), auditory (voice) recognition and also includes chemical, behavioural and olfactory analysis.[28] It is already being used by private firms to verify identities. As with any identification procedure privacy is an issue and Standards Australia advised that Codes of Ethics are being development by the Biometrics Institute for this purpose.[29]

4.45 The Attorney General's Department told the Committee that the Criminal Code includes specific fraud offences.[30] Identity fraud is a feature of welfare and tax fraud offences, along with increasingly being featured in organised crime. The Department also advised that it is developing a strategic direction for improved personal identification and authentication practices. For example, the AUSTRAC Proof of Identity Steering Committee is assessing the community cost of identity fraud. The steering committee includes representatives from the banking industry as well as government agencies.

4.46 In addition, the ACC has maintained the Identity Fraud Register which lists known offenders, fraudulent names used and lost or stolen documents. The Australian Bureau of Criminal Intelligence (ABCI) established this project in 2001, and the ACC submission indicates that over 2000 recent fraudulent identities have been recorded on the database. The database can link offenders with real identities and crimes and is designed to facilitate the work of law enforcement agencies (LEAs).[31] The Committee commends this initiative.

4.47 The Committee encourages the continuation of the close working relationship between the banks and the police – both state and federal.[32] Cross sector liaison is essential for the sharing of information and the development of strategies to minimise the effect of cybercrime.

4.48 However, as was indicated in the evidence provided by Symantec, the implementation of strategies and technology depends upon the cost of the technology and persuading people to use it.

> … you have to make this cost-benefit analysis and if the financial institutions in a particular country have decided that there is an acceptable level of risk with a technology they are using, they are going to continue with that technology.[33]

---

28 http://www.biometricsinstitute.org/bi/types.htm

29 *Committee Hansard,* 18 July 2003, p. 53

30 Submission no. 21, p.13

31 Submission no. 23, p.24

32 *Committee Hansard*, 18 July 2003, p. 43

33 *Committee Hansard*, 18 July 2003, p. 80

4.49 The Committee is disturbed at the notion of 'an acceptable level of risk' for the financial institutions. What is acceptable to the banks may not be acceptable to the consumers of the financial services provided. Where such an acceptable level has been determined, the consumers should at least be made aware of it and advised as to what they can do to minimise that risk.

Money laundering

4.50 Money laundering is defined by the OECD as:

> The processing of … criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.[34]

4.51 In evidence the Committee heard that the OECD's associated Financial Action Task Force is an intergovernmental initiative whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

4.52 The ACC advised the Committee that money laundering is one of the areas in which the Commission is authorised by the Board to use its coercive powers, along with associated criminal activities of South-East Asian crime gangs, established criminal networks and illegal firearms.[35]

4.53 The Australian Bankers' Association told the Committee of its very strong relationship with AUSTRAC. The banks, under the *Financial Transactions Reports Act 1988*, are required to report suspicious transactions to AUSTRAC, and the Association indicated that in addition to matters arising from traditional crime and money laundering, there is now also a focus on the suppression of the financing of terrorists.[36]

4.54 AUSTRAC's evidence noted its role as an observer and reporter on international funds transfer instructions or international telegraphic transfers. The agency has been turning its attention to what happens outside of the regulated financial markets, and the potential for the expansion of unregulated financial transactions.[37]

4.55 AUSTRAC advised the Inquiry that the AGEC (Action Group into the Law Enforcement Implications of Electronic Commerce) which is chaired by AUSTRAC, has also been examining this area in two of its focus groups: one on new technologies and the other on the financial system. The Group's membership includes the Australian Taxation Office, the Australian Federal Police, the

---

34 OECD website http://www1.oecd.org/fatf/MLaundering

35 *Committee Hansard,* 18 July 2003, p. 6

36 *Committee Hansard*, 18 July 2003, p. 36

37 *Committee Hansard*, 18 July 2003, p. 55

Commonwealth Attorney-General's Department, the Australian Competition and Consumer Commission, the Australian Securities and Investments Commission, the Australian Customs Service, the Director of Public Prosecutions, the Department of Immigration, Multicultural and Indigenous Affairs, and the Australian Prudential Regulation Authority.

4.56 AUSTRAC explained:

> [The AGEC is] looking at ways of avoiding the financial system … E-gold and other similar types of mechanisms have been of great interest, particularly to the Australian Taxation Office. People use them to avoid our reporting mechanisms … on international funds transactions. It is quite easy to use these mechanisms by buying e-gold and then having credit cards or debit cards on international accounts so that our reporting systems are completely avoided. There is quite a large amount of concern within the broader law enforcement agencies, including revenue and regulatory agencies, about those sorts of mechanisms.[38]

4.57 The Committee learned that such systems are simple to use, and can effectively transfer large sums undetected to and from Australian–owned 'accounts'.

Prevention – Money Laundering

4.58 In addition to the establishment of the AGEC Committee, the Committee was advised of other technical and strategic resources available to deal with money laundering.

4.59 The Attorney General's Department told the Committee that there are strategies available to combat money laundering. The threat of terrorism has given money laundering a new global focus apart from its traditional connection with organised crime.[39]

4.60 The Department also informed the Committee that Australia is a member of the international Financial Action Task Force on Money Laundering (the FATF), which has developed the Forty Recommendations – the basis of international anti-money laundering standards, which include sanctions against non-compliant countries.

4.61 Post 11 September 2001, the FATF released eight Special Recommendations on Terrorist Financing, accompanying the United Nations measures. A review of the Forty Recommendations is currently under way.

4.62 In 1997, the Asia Pacific Group on Money Laundering (APG) was established as a FATF-style regional body of 26 member states. The APG plays a

---

38 *Committee Hansard*, 18 July 2003, p. 58

39 Submission no 21, p.13

coordinating role in the provision of technical legal and law enforcement experts to countries in the region.

4.63 In addition to the *Financial Transactions Reports Act 1988,* money laundering, in the domestic arena, is managed within the framework of the *Proceeds of Crime Act 2002*. Under this legislation courts can freeze and confiscate assets under certain circumstances.

4.64 There is also state-based proceeds of crime legislation, which allow civil forfeiture of assets, in state offences. The ACC has frequently used this legislation to recover proceeds of crime, and under the Commonwealth legislation is in a position to assess the effectiveness of the *Proceeds of Crime Act 2002* in recovering laundered funds, and whether it is at all useful in recovering funds which have been transferred outside the reporting system.

Future directions for banking, credit card fraud and money laundering

Australia a vulnerable target

4.65 The ACC submission notes that there are limitations in the Australian national law enforcement's response to card skimming which can be exploited by being open to criminal activity. Further, the ACC considers that the increasing controls over card skimming activity in North America, Europe and Asia, and the lax legislative (multi-jurisdictional in one country), and deterrent environment is likely to result in transnational criminal groups shifting their activities to Australia.[40]

4.66 The ACC notes[41] a report in September 2002, by the Office of Strategic Criminal Assessments[42] (OSCA – now incorporated into the Australian Crime Commission) which predicted that the threat of card skimming would continue to rise, and cited a number of contributing factors. These included legislative gaps such as restrictions on the import of skimming equipment such as card blanks and skimmers; lack of jurisdictional agreement on what constitutes an offence, and lack of deterrence factors in criminal penalties.

4.67 OSCA also cited:

- systemic weaknesses in banking practice (such as lax merchant practices);
- lack of consumer awareness of card security;
- a gap in Australian law enforcement intelligence holdings; and
- an acknowledged need for a national intelligence gathering strategy.

---

40 Submission no 23, pp.27-28

41 Submission no 23, p.30

42 OSCA, *Fraud – Credit Card Skimming,* No. 02/02 September 2002

4.68 In the Committee's view, the ACC can make a significant contribution to the gap in intelligence holdings and the development of a national intelligence gathering strategy. OSCA, as part of the ACC is in a position to provide information on cyber fraud and related activity to law enforcement and policy bodies on a regular basis. The Committee notes that one of the strategies that the ACC identified as contributing to a national response included the provision of a national intelligence database on card skimming for enhanced intelligence exchange. It notes that this role would fill a gap in current law enforcement arrangements on card skimming.[43]

4.69 The Committee is of the view that this role should be expanded. During the Inquiry, it formed the view that there was the potential for inter-relationships between the various forms of banking cybercrime and that this potential should be explored.

Recommendation 6

The Committee recommends that the Australian Crime Centre, in consultation with the Australian High Tech Crime Centre (AHTCC), Austrac and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.

4.70 In relation to consumer awareness of card security, the Committee notes that the ABksA considers that the Government has a role in public education programs to ensure that customers understand their responsibilities. Given the significance of banking in a community's economic health, the Committee believes it is necessary for government and financial institutions to form partnerships to support increased client awareness of the potential pitfalls.

4.71 The issue of the systemic weakness in banking practice may be overcome in part by education campaigns. The Committee notes that that the AHTCC advised that in May 2003, the AFP, AusCERT and other law enforcement agencies produced the *Australian computer crime and security survey*.[44] The AHTCC indicated the survey showed that:

- corporations are spending more money on IT security aspects; but also
- there are certain generic vulnerabilities within some industries.

4.72 These vulnerabilities demonstrate that there is a need for firewalls, intrusion detection systems and policies to prevent contamination from disks imported from outside an organisation's system.

4.73 In addition the AHTCC, Standards Australia and the Attorney-General's Department, have funded the production of a computer forensics guide for industry.

---

43 Submission No. 23, p. 32

44 *Committee Hansard*, 21 July 2003, p. 22

This is an evidence collection guide designed to advise the industry on how they may start protecting themselves gathering together the information that is needed to prosecute these matters effectively.

4.74 In his evidence to the Committee, Mr Orlowski referred to a number of potential solutions for protecting identity, and thereby eliminating some of the aspects of banking and credit card fraud. These include public key technology:

> which is a very strong security tool based on cryptography and which is seen as the cornerstone for electronic commerce in providing secure and authenticated electronic transactions.[45]

4.75 There is also the strengthening of technology through the use of smart cards which would mean that a person wanting access to another's data would require the card to do it, as it would be 'computationally infeasible' to break the information.[46]

4.76 Other technology which has potential in this area is biometrics (discussed in detail at paragraph 4.43). However, the NSW Police pointed out to the Committee that biometrics – for example, biometric links to credit data – as a security solution are really a matter of what the community will tolerate.[47] The Committee is aware of the sensitivity surrounding centralised access to personal data, and that there are compromises to be made if biometrics becomes the technology of choice.

4.77 The NSW Police also noted the overseas experience in which telephone lines are physically intercepted to pick up data. If at any point along the communication lines the data is not encrypted it has the potential to expose millions of users to capture or corruption of data.

4.78 The implications of failure to secure data are widespread. Not only could financial details be captured, but other personal and corporate material taken and used. The detection is difficult and resource intensive and there is also potential for civil litigation for those who suffer loss through no fault of their own. While it is a Commonwealth offence to intercept telecommunications without a warrant, there would also be offences arising out of the corruption or use of the data for gain or benefit. It is clear that law enforcement agencies should devise prevention and response strategies, in the event that telephone line intercepts occur in Australia. In particular, the ACC in partnership with the AHTCC is in a position to develop response strategies, based on its operational experience.

4.79 The Committee notes that in relation to credit card fraud, and in particular card skimming, the ACC considers that it has a role: its submission to the Inquiry indicates:

---

45 *Committee Hansard* , 17 July 2003, p. 2

46 *Committee Hansard*, 17 July 2003, p. 8

47 *Committee Hansard*, 18 July 2003, p. 88

> Although many of the specific offences associated with card skimming are fraud under State Criminal Codes, card skimming is appropriately regarded as federally relevant criminal activity and will require priority attention from national law enforcement.[48]

4.80 The ACC also advises that its contribution to a national response to this problem could include a series of strategies:

- focusing on the multi-jurisdictional and national dimensions of card skimming;
- utilising specialist financial investigation resources to complement the expertise of partner agencies;
- using cybercrime investigation methods and forensic techniques;
- providing enhanced insight into the problem and undertaking intelligence collection and target development; and
- contributing to appropriate legal, administrative and policy responses.[49]

4.81 The Committee notes that many of the strategies are activities that the Committee views as being part of the ACC's normal range of activities, for example, the last item 'contributing to appropriate legal, administrative and policy responses.'

4.82 Given that the submission indicates that in May 2003, the ACC board approved National ACC 'Intelligence Operations' for both Identity Crime and Card Skimming[50] the Committee would be expecting the Commission to be more positive in its strategic planning for this growth area.

4.83 Similarly, in the areas of money laundering and identity fraud, the ACC continues to pursue traditional strategies. Their suggested future directions include a large number of continuing activities such as consultations with AUSTRAC and the banks, in particular concerning the FATF's 40 recommendations, the use of Task Forces such as the Agio task Force, continuation of the work with AGEC and the former ABCI Identity Fraud register, and continued involvement in consultations concerning verification of identity documents. The more innovative suggestions include the establishment of a Task Force to investigate identity fraud.

4.84 While the Committee does not discount the effectiveness of traditional strategies the growth of crime in cyberspace suggests that to successfully combat it, LEAs may need to demonstrate a willingness to undertake new initiatives.

4.85 The Commission also mentions investigative techniques to include use of ACC Special Powers for production of documents and examination of witnesses. The Committee notes the special authorisation of the ACC Board for inquiries of this

---

48 Submission no.23, pp. 31-32

49 Submission no 23, p. 31

50 Submission no 23, p. 32

nature, but is apprehensive that these powers may be extended and become more commonplace than was initially envisaged.

Conclusion

4.86 The Committee notes that there is significant work being done on the international as well as the domestic level to minimize banking and credit card fraud, and to deal with money laundering. As with other aspects of cybercrime, there are two issues:

- education – to ensure the private and public users of this technology are aware of the risks and take steps to minimise them; and
- overall co-ordination and dissemination of relevant and timely information to the agencies involved.

4.87 The Committee considers that the proliferation of working parties, focus groups, interagency committees and similar groups has the potential to be more effective if there is an agency which can act as a co-ordinator of information and direct resources appropriately.

4.88 There is clearly a need to update the legislative base, which the Committee understands is occurring. The process should not stop at updating, as constant review is what is required to ensure that there is the ability to deal with the latest incarnation of attempts to damage the banking and finance environment.

4.89 Success in the detection and prosecution of cybercrime will depend on cooperation between Commonwealth and State Law Enforcement agencies, the financial institutions, as well as other agencies (such as AUSTRAC). The Committee considers that the formation of partnerships between these parties is crucial, if banking and monetary cybercrime is to be dealt with efficiently. In particular, government and private sector partnerships should be sought to disseminate important information regarding protection from financial fraud.