Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:19
Received 19 May 2003
Mr Tony Burke
Director
Australian Bankers' Association
Level 3
56 Pitt Street
SYDNEY NSW 2002
☎02 8298 0409 02 8298 0402
E-mail: tburke@bankers.asn.au

AUSTRALIAN BANKERS' ASSOCIATION SUBMISSION

Cybercrime Inquiry

Table of Contents

1. Introduction 7

2. Scope of Report 8

3. Environment and Industry Analysis 9

3.1 Non-Financial Crimes 9

3.1.1 Child pornography 9

3.1.2 Theft of information and telecommunication services 9

3.1.3 Communication in furtherance of criminal conspiracies 10

3.1.4 Telecommunications piracy 10

3.1.5 Dissemination of offensive materials 10

3.1.6 Electronic vandalism and terrorism 10

3.1.7 Illegal interception of telecommunications 11

3.1.8 Other 11

3.2 Financial Crimes 11

3.2.1 Credit card fraud: 11

3.2.2 Debit card fraud 14

3.2.3 Money laundering/ terrorist financing 16

3.2.4 Cybercrime relating to Internet banking facilities 20

3.2.5 Identity theft 21

3.2.6 Securities and investment fraud 22

3.2.7 Sales and Investment Fraud 23

3.2.8 Other 25

3.3 Summary of current industry responses to the threat of cybercrime 25

3.3.1 Education 25

3.3.2 Risk management 25

3.3.3 ABA Fraud Taskforce 27

3.3.4 Government Collaboration 27

4. Critical Infrastructure Protection 29
4.1 Definition: 29
4.2 Industry interdependency 29
4.3 Current Government response: 29
4.4 Banking Sector approach 30
5. Legal Analysis 31
5.1 Legislative Framework that Impacts upon Cybercrime 31
5.1.1 Criminal Code Act 1995 (Cwth): 31
5.1.2 Cybercrime Act 2001(Cwth) 32
5.1.3 Privacy Act 1998 (Cwth) 32
5.1.4 Proceeds of Crime Act 2002 (Cwth) 33
5.1.5 Financial Transactions Reporting Act 1990 34
5.1.6 Payment Systems Regulation Act 1998 34
5.1.7 Mutual Assistance in Business Regulation Act 1992 34
5.1.8 Telecommunications Act 1997 35
5.1.9 Telecommunications Interception Act 1979 (Cwth) 35
5.1.10 Australian Crime Commission Act 2002 36
5.1.11 Charter of the UN Act 1945 (Cwth) 36
5.1.12 Banking Act 1959 (Cwth) 36
5.2 Self regulation and co-regulation 37
5.2.1 Code of Banking Practice 38
5.2.2 EFT Code of Practice 38
5.2.3 Australian Payments Clearing System (APCA) 38
5.3 Liability issues 39
6. Recommendations 40
Appendix A: Details of Measures Adopted by Banks 43
Appendix B: Examples of Education Programs Relating to Cybercrime 55

Appendix C: Theft of Information and Telecommunications Services 58
Appendix D: Card Skimming 60
ABA Consumer Tips 63
Appendix E: FATF Recommendations 65
General Framework of the Recommendations 66
Appendix F: State Legislation 73
Appendix G: Code of Banking Practice 1993 76
Appendix H: Product Information 87

1. Introduction

The Australian Bankers' Association (ABA), the peak body for banking in Australia, is pleased to contribute to the Parliamentary Joint Committee on the Australian Crime Commission's inquiry into cybercrime, established under section 55(1)(d) of the *Australian Crime Commission Act 2002*.

Banks are among the largest users of telecommunications facilities in Australia. They use the Internet for banking transactions such as payment of bills and transfers of funds between accounts. Many other types of retail banking transactions occur through Automatic Teller Machines (ATMs) and Electronic Funds Transfer at the Point of Sale (EFTPOS) devices that are connected via telecommunication networks. Wholesale, inter-bank and international banking transactions are conducted on dedicated telecommunication networks.

Banks also collect and store huge volumes of account and customer information, which can be accessed via telecommunication services.

In summary, the ABA's position is that:

1. The current regulatory framework covering cybercrime is satisfactory and no further legislation or regulation is required at the Commonwealth level.

2. 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.

3. 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.

4. 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.

2. Scope of Report

For the purposes of this submission, the ABA has adopted the following definition of "cybercrime":

> ***"A cybercrime is any crime effected or progressed using a public or private telecommunications service".***

This submission does not address in detail all of the terms of reference of the inquiry, and raises other matters which are not included in those terms. The submission addresses the issues that most affect ABA members.

3. Environment and Industry Analysis

3.1 Non-Financial Crimes

The Internet, in combination with other telecommunication networks, has developed into a major commercial infrastructure, which has in turn attracted the attention of the criminal community. The banking sector has rapidly changed to take advantage of this new environment and has had to deal with new issues and threats.
In relation to cybercrime, a distinction may be made between financial crimes and non-financial crimes. Non-financial crimes are crimes that do not involve a financial loss and include offences such as child pornography, computer hacking, smuggling of people, trafficking of drugs, extortion and trafficking in counterfeit goods.
Following are some of the non-financial cybercrimes that the ABA has defined[1]. It is not to be taken as an exhaustive list, as new categories of crime continue to be identified.

3.1.1 Child pornography

This issue is outside the scope of this submission.

3.1.2 Theft of information and telecommunication services

Information services theft is the unlawful use of an information service or communications service, or the manufacture, sale or supply of equipment that can be used for information services theft. It has in the USA become a major problem for cable TV providers, and other information providers such as value added information services. Some States in the USA have enacted specific legislation to deal with the problem[2].

Telecommunications theft involves the unauthorised tampering with telecommunications equipment to gain free telephone calls[3].

These issues not only affect ABA members, but also have the potential to concern all users of telecommunications services. ABA members treat the issue of information theft very seriously and implemented appropriate risk management mechanisms to minimise the risk of theft of commercial information.

---

1 For an expansive discussion on non-financial and financial crimes see. Grabosky, P N & Smith, R G 2003, 'Crime in the Digital Age', in A Goldsmith, M Israel & K Daly (eds), *Crime and justice: an Australian textbook in criminology,* 2nd ed, Lawbook Co., Sydney, pp. 179-99

2 See for example the State of Nevada legislation in Appendix B

3 Grabosky, P., "Computer Crime in a World without Borders", Journal of the Australian Federal Police "Platypus", June, 2000 http://www.afp.gov.au/raw/Publications/Platypus/Jun00/compcri.htm

3.1.3 Communication in furtherance of criminal conspiracies

This crime involves the use by criminal groups of telecommunication services to communicate and organise their criminal activities[4]. Although this is a serious problem, it is not addressed in this submission.

3.1.4 Telecommunications piracy

Piracy involves the infringement of copyright material through the use of telecommunications facilities. This has become a major crime through the advent of peer-to-peer systems such as Napster, Morpheus and Kazaa. The Recording Industry Association of America believes that the cost of peer-to-peer networks to the recording industry amounts to many millions of dollars per year[5]. The first case in Australia (and one of the first in the world reported) concerning telecommunications piracy was determined on 13 May 2003 by the New South Wales Downing Centre Local Court. The court held that 3 students were guilty of copyright infringement through the use of a Napster-like website that they were operating.

Although this is a serious problem, it is not addressed in this submission.

3.1.5 Dissemination of offensive materials[6]

There are materials other than child pornography that are offensive and abundant on the Internet. Such material includes other sexually explicit material, racist propaganda and instructions to build explosive and dangerous devices[7].

This issue is outside the scope of this submission.

3.1.6 Electronic vandalism and terrorism

This category concerns hacking and other unauthorised access to computer systems for no financial gain. Hackers are often motivated by thrill seeking, politics, or simple malice, rather than an intention to gain financial rewards.

---

4 Grabosky, P., ibid

5 http://www.riaa.com/Protect-Online-1.cfm

6 "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet", A Report of the President's Working group on Unlawful Conduct on the Internet, March 2000. http://www.cybercrime.gov/unlawful.htm

7 ibid

Banks are fully committed to fulfilling their responsibility in the protection of Australia's Critical Infrastructure, including defences against vandalism and terrorism. This subject will be discussed further below.

3.1.7 Illegal interception of telecommunications

This category includes the unauthorised interception of telecommunications under the *Telecommunications Interception Act 1979*.[8]

Illegal interception may have a financial objective (and so, becomes a financial crime). The incidence of this type of crime is growing overseas, but is not addressed further in this submission.

3.1.8 Other

Other categories of non-financial cybercrime include:

a) cyberstalking;

b) spamming;

c) illegal Internet gambling;

d) sale of prohibited goods via the Internet

e) procuring a person under 16 to engage in sexual activity[9]

3.2 Financial Crimes

Financial crimes are crimes that involve a financial loss to at least one of the parties to the event or activity, and include such crimes as credit card fraud, debit card fraud money laundering and corruption (with or without coercion).[10]

3.2.1 Credit card fraud:

3.2.1.1 Definition:

Credit card fraud is any activity whereby:

[8] There appears to exist a substantial anomaly with the Telecommunications Interception Act 1979 that is more fully discussed in Section 5 below.

[9] See Section 218A of the Queensland Criminal Code

[10] http://www.interpol.int/Public/FinancialCrime/Default.asp

(a) a third party (not the legitimate holder of the credit card) falsely uses a credit card or information about a credit card for any purposes not authorised by the legitimate holder of the credit card; or

(b) the legitimate holder of the credit card falsely uses the credit card allocated to them for a purpose not authorised by the issuer of the credit card.

3.2.1.2 Current issues:

There are a number of ways by which the fraud can be accomplished, including:

(a) fraudulent use of lost or stolen cards;

(b) the making of a fraudulent application;

(c) the creation of a counterfeit card, which can be achieved either through the process known as skimming or through the use of white plastic;

(d) the intercepting of cards in the mail system;

(e) Card Not Present (CNP) fraud, in relation to telephone or Internet credit card transactions;

(f) making multiple imprints from a credit card during a single transaction.

CNP fraud is a significant risk in the cybercrime field. Under the "Card Not Present" (CNP) rules the merchant is able to process an online or telephone purchase provided they obtain some basic information about the relevant credit card:

(a) Credit card number;

(b) Name of card holder;

(c) Name of issuer;

(d) Expiry date[11].

All of this information is embossed on the credit card. From a security perspective the process is low cost, but relatively high risk. Rules have been developed by and for the banking sector to protect all parties to a transaction.[12]

[11] See http://www.usa.visa.com/business/merchants/fraud_basics_cardnotpresent.html

[12] The card schemes developed the MOTO rules (mail order/telephone order rules) that apply in all non face-to-face transactions.

A merchant accepting a credit card to process a CNP transaction forwards the captured information to the merchant's bank. The merchant's bank credits the merchant's account with the value of the transaction and then attempts to extract payment from the alleged customer. If the merchant's bank cannot obtain the value of the transaction from the alleged customer, the bank applies a "charge back", whereby the merchant's bank account is debited the value of the disputed transaction and a small administration fee.

For a CNP purchase, the merchant does not have any documentary evidence to support the transaction that can be forwarded to their bank. The alleged customer does not have any contractual relationship with the merchant's bank (in respect of the CNP transaction) and the merchant's bank will encounter substantial legal difficulties in the enforcement of payment

There is only a contract between the merchant and the customer and it will be the merchant's responsibility to seek restitution directly from the alleged defaulting customer

3.2.1.3 Impact:

The impact of credit card fraud (including CNP fraud) on banks and other financial institutions has been substantial. The market has demanded banks provide a payment system that can be used conveniently via telecommunications services. This has led to an increase in credit card fraud, and this has caused banks substantial investigation and restitution costs. In many cases these costs are either not recoverable or only partially recoverable.

As is the case with other types of cybercrime, there are many victims of credit card fraud other than banks, and there are very large non-financial impacts. However, in terms of direct costs, the banking sector is absorbing a large share of the burden, at the same time as shareholders expect sustained and improving financial performance, and all Australians wish to continue to enjoy the benefits of a healthy banking sector.

3.2.1.4 How banks are addressing the issue:

Key measures undertaken by banks include:

- Prevention. Customer and merchant education, authorization processes and merchant card acceptance procedures.
- Detection. Fraud detection tools for monitoring spending and merchant activity patterns; exception reporting; behavioural analysis.

- Investigation. Specialist in-house investigation teams; liaison with law enforcement agencies and card schemes.

Education is of crucial importance, and the task of informing and educating the community should however be undertaken by all stakeholders including those government agencies concerned with consumer protection[13].

ABA members are currently working closely with NSW Police on Strike Force Venlo, which is specifically targeting credit card fraud in NSW. A number of successful investigations and prosecutions have already been concluded.

See Appendix A for further detail on measures undertaken.

3.2.2 Debit card fraud

3.2.2.1 Definition:

Debit card fraud is any unauthorised activity regarding a debit card and includes:

(a) the production and use of counterfeit debit cards;

(b) the stealing of legitimate debit cards.

3.2.2.2 Current issues:

There are a number of ways by which debit card fraud can be committed, including:

(a) fraudulent use of lost or stolen cards;

(b) the making of a fraudulent application :

(c) the creation of a counterfeit card (skimming);

(d) the intercepting of cards in the mail system;

In each case, the fraudster will also require the PIN for the account to which the card pertains.

Skimming is a relatively new form of fraud (for both credit and debit cards) and is being addressed by banks as a significant cybercrime threat.

[13] For example, both ASIC and the ACCC have established websites that deal with consumer related cybercrime issues.

It involves the legitimate cardholder handing the card to a third party for a legitimate transaction. The third party (the fraudster) uses a device (a skimmer) to copy the information encoded on the magnetic stripe on the reverse side of the card. The fraudster can then produce counterfeit magnetic stripe cards that are in effect the same as the original card. If the fraudster can obtain a PIN then the counterfeit cards can be used for debit card transactions.

Skimming can be accomplished by a variety of means, including the use of covert readers and devices concealed in false ATM components. [14]

3.2.2.3 Impact:

The use of counterfeit cards not only has a substantial financial impact upon customers but also substantially increases bank investigation and detection costs.

3.2.2.4 How banks are addressing the issue:

Key measures undertaken by banks include:

- Prevention. Customer and merchant education, authorization processes and merchant card acceptance procedures.
- Detection. Database interrogation to identify common points of purchase; exception reporting; surveillance at ATMs.
- Investigation. Specialist in-house investigation teams; liaison with law enforcement agencies and card schemes.

The most effective mechanism to address debit card fraud is educating customers on the risks involved. ABA members will continue to provide information on techniques to greatly reduce the risk of skimming and other threats, but as with credit card fraud, the assistance of government agencies and other stakeholders is required.

See Appendix A for further detail on measures undertaken.

[14] See Appendix C for a further detailed explanation of card skimming.

3.2.3 Money laundering/ terrorist financing

3.2.3.1 Definition:

Money laundering can be defined generally as the process of concealing the existence, illegal source, or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate. Deception is the heart of money laundering: deceiving the authorities by making assets appear to have been obtained through legal means with legally-earned income, or to be owned by third parties who have no relationship to the true owner[15].

3.2.3.2 Current issues:

One of the real difficulties in dealing with money laundering is the sophistication that the criminal community displays in hiding their activities. It is often difficult to follow financial trails of evidence. In Australia this is made more difficult because there is no uniform evidence regime. Apart from the Commonwealth and New South Wales, no other jurisdictions have adopted the *Uniform Evidence Act*. The lack of uniform evidence regime in Australia requires banks to have different procedures covering each jurisdiction's evidence requirement in the event of a cybercrime prosecution.

The *Financial Transactions Reporting Act (Cwth)* (FTRA) has assisted in the monitoring of financial transactions. One of the difficulties in practice is that the banks complying with FTRA - in opening accounts for example - rely on the documents presented as having been validly issued.

In opening a bank account the potential customer must present documents that fulfill the "100 point check" as required under the FTRA. The primary documents can be a passport, a birth certificate or a certificate of citizenship. Each of these documents account for 70 points. The potential customer must also present secondary documents in order to reach the minimum 100 points requirement. These documents include drivers license (40 points), public employee or student ID card (40 points), credit card (25 points), Medicare card (25 points) and Council rates notice (25 points).

The Banks are dependent on government issuing agencies complying with their own guidelines and legal obligations in the issuing of the primary documents. This issue has been raised previously with Government agencies and it must be recognized that if the documents have not been validly issued

[15] US Department of State, 1997 International Narcotics Control Strategy Report, March 1998, http://www.hri.org/docs/USSD-INCSR/97/Financial.html

by the relevant government agency then it is possible for the bank to open an account that may be used for money laundering or other unlawful use.

In relation to money laundering and the suppression of financing of terrorism, Australian banks have accepted the new compliance burdens leading from Australia's adoption of the Financial Action Task Force (FATF) Recommendations, and the US Patriot Act, as well as Australian legislation, but need Government support in ensuring pragmatic solutions can be found to compliance issues, and in working with global bodies such as the OECD to have uniform international standards for risk management and regulatory compliance systems and processes.

A recent trend is for those involved in money laundering to take advantage of "alternative" financial transaction systems (not under the control of Australian banks), such as E-Gold.

3.2.3.3 Impact:

There is no effective way to accurately estimate how much money is being laundered via telecommunications services. In 1997, the Australian market generated approximately 1.5 billion electronic transactions. This included both credit and debit card transactions. It has been estimated that of these transactions, Internet transactions only accounted for $55 million[16].

If the growth rates for Internet transactions have continued since these figures were published, it is estimated that Internet transactions in Australia for the year 2002 will account for approximately $900 million of which $16 million approximately could be laundered money[17]. This is almost certainly a small proportion of the value laundered via all telecommunications services.

Failure to adequately address money laundering activities adequately has an impact at different levels. The impact at community level is that criminals and terrorists are able to finance their activities and enjoy ill-gotten gains. The impact for banks is on reputation and credibility, and sanctions if they are caught (wittingly or unwittingly) laundering money for organized crime, or moving terrorist funds. Banks also face the costs of compliance. Legitimate businesses and individuals may also suffer financial and other losses.

---

16 Walker, J., "Laundering on the internet : an economic model for forecasting online flows of dirty money", http://members.ozemail.com.au/~born1820/Trento2.html

17 Ibid

3.2.3.4 How banks are addressing:

In 1990, the OECD published its FATF report on money laundering, which made Forty Recommendations aimed at addressing the problem of money laundering. Australia has been a member of FATF since its inception, and currently 130 countries including Australia have endorsed the Forty Recommendations. A copy of the Forty Recommendations is attached at Appendix D.

The Forty Recommendations are recognized as the leading international standard for anti-money laundering. The FATF is completing a review of the Forty Recommendations, and 8 new Special Recommendations, to ensure that they adequately address changes in money laundering methods and trends, as well as the international developments such as the UN Transnational Organized Crime Convention and the Terrorist Financing Convention. The new Recommendations are expected to be ratified in June 2003.

Additionally, the revised Recommendations will take into account FATF's recently expanded mission in combating terrorist financing and will ensure that its revised framework provides for measures to deny terrorists access to the international financial system.

According to the OECD, Australia has approached the issue of anti-money laundering regulation in a well-balanced manner. In particular the OECD has indicated that[18]:

> *"The Australian Government has adopted a "whole system" approach to dealing with money laundering by putting in place appropriate law enforcement structures, legislation and operational techniques. Australia has taken the FATF philosophy and extended it to areas such as money laundering associated with tax evasion and extending the cross-border reporting requirements to international wire transfers. The Australian system gives high priority to the use of financial reports and related information to locating the money trail, particularly with regard to organised crime and serious criminal offenders. In this respect, the Australian Government has established AUSTRAC (Australian Transaction Reports and Analysis Centre), a specialised regulatory agency to work with the financial sector, to receive reports of significant and suspicious transactions and to analyse financial transaction data. That data in the form of intelligence is made available to Australia's major law enforcement agencies and the*

[18] http://www.fatf-gafi.org/Ctry-orgpages/ctry-au_en.htm#Legislation

> *Australian Taxation Office (ATO) to assist them in their actions against criminal activity and tax evasion.*
>
> *A major feature of the Australian use of financial transaction data is the operation of a Task Force of agencies. The members include the Australian Bureau of Criminal Intelligence (which represents the States and Territories), the Australian Customs Service, the Australian Federal Police, the Australian Taxation Office, AUSTRAC and the National Crime Authority. This process ensures that information of importance is quickly and efficiently distributed to relevant law enforcement agencies… It has particular importance in the investigation of organised criminal activity but also assists in dealing with major tax avoidance and in uncovering practices which seek to defeat the reporting obligations of Australian law.*
>
> *The Australian system has matured significantly since the first evaluation which was conducted in March 1992. AUSTRAC has grown in importance and effectiveness. In this regard, it is to be commended for its untiring efforts in working closely with the financial sector, in receiving and analysing financial transaction data and in providing the data in the form of intelligence to the appropriate agencies. …*
>
> *… Australia can pride itself on a well-balanced, comprehensive and in many ways exemplary system, and must be congratulated accordingly. It meets the objectives of the FATF Recommendations and is constantly reviewing the implementation of their anti-money laundering provisions, simultaneously looking well ahead in the future. Of course, there is always room for improvement, but most of the weaker points of the system -- such as they control of the bureaux de change, the reliability of the identification and the extension of the FTR requirements to other operators such as solicitors -- have already been identified by the Australian authorities and are under consideration."*

The banking sector will continue to work closely with AUSTRAC on cybercrime and anti-money laundering, as these are issues of critical importance to the integrity of the banking sector.

The FATF conducts evaluations of member and non-member countries' and territories' compliance with their Recommendations. Australia is one of the 29 FATF members, and considers itself to be fully compliant with the 40 Recommendations. However, the FATF assesses Australia to be fully compliant with 38, (partially compliant with 2), of the 40 Recommendations.

Australia complies with the requirement that supervised institutions have adequate programs in place to guard against money laundering. However,

these programs are not currently statutory requirements under Australian banking laws. Australian authorities are able to cooperate and lend expertise to other domestic judicial or other law enforcement authorities 'on request', but not 'spontaneously' as required by the FATF.

There has been good cooperation between banks, and with government agencies on the handling of suspicious transactions and proscribed persons and entities.

See Appendix A for further details of measures undertaken.

3.2.4 Cybercrime relating to Internet banking facilities

3.2.4.1 Definition:

This category includes:

(a) the unauthorised access;

(b) unauthorised modification; or

(c) unauthorised impairment

of Internet banking facilities[19].

3.2.4.2 Current Issues:

Obviously, Internet banking facilities are attractive targets for criminals. In general terms, Internet banking sites require the account number, followed by some password security mechanism. 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.

3.2.4.3 Impact

Any failure in the security of a bank's Internet banking facility can substantially undermine the market's trust in that facility. A central goal of modern banking is to ensure that proper security mechanisms are in place so that the market has confidence in utilising the bank's services. If there is an undermining of this confidence, this may have a substantial adverse affect

[19] Section 477 *Cybercrime Act 2001 (Cwth)*

not only on the bank's ability to retain its customers and its market value, but also on the stability of the banking system as a whole.

3.2.4.4 How Banks are addressing

The banking sector has made very large investments on technological and other solutions to ensure that there is market confidence in using Internet banking facilities. These solutions are not limited simply to the use of firewalls or intrusion detection systems, but include highly sophisticated heuristic software packages that monitor the access to their facilities so as to better identify any attempted unauthorised access.

3.2.5 Identity theft

3.2.5.1 Definition:

Identity theft occurs when someone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of Commonwealth law, or that constitutes an offence under any applicable State law.[20]

3.2.5.2 Current issues:

Identity theft is one of Australia's fastest growing crimes and the increasing incidence of identity crime is likely to not only impact on Australia's economy, but on consumer confidence in areas such as electronic commerce. As with the USA, Australia faces some difficult regulatory challenges posed by its federal structure, and has no national identity card that could be used to regulate identities.

Medicare cards, passports, and the electoral roll are all administered by different Commonwealth Departments, and the different States and Territories issue and administer their own drivers' licences and births, deaths and marriage certificates.

Banks are unable to authenticate many of the identity documents stipulated for use under the *Financial Transactions Reporting Act.*

A further issue is the ready availability of inexpensive technology enabling fraudsters to produce convincing, false identity documents.

[20] http://www.usdoj.gov/criminal/fraud/idtheft.html

3.2.5.3 *Impact*

The estimated cost of identity theft in Australia is in excess of $2 billion per annum, and identity fraud constitutes about one third of all fraud complaints to the Australian Federal Police annually.[21]

This figure, on the experience of other developed economies such as the USA, is expected to increase. Identity theft complaints in the USA, according to the US Federal Trade Commission, ranked as the number one complaint for the third year in a row in 2002, with 161,819 reported instances, up 88 percent from the previous year's figure of 86,198, and constituting 42% of all consumer fraud complaints made to the Commission. Banking fraud accounted for 17 percent of identity fraud complaints.[22]

3.2.5.4 *How banks are addressing*

Key measures undertaken by banks include:

- Prevention. Customer and merchant education; 100 point check; comparisons with databases of fraudulent identities.
- Detection. Online verification; fraud detection tools; electronic white pages
- Investigation. Specialist in-house investigation and risk management teams; liaison with law enforcement agencies.

Education is the most effective mechanism to prevent identity theft, and all stakeholders must contribute.

See Appendix A for further detail on measures undertaken.

3.2.6 Securities and investment fraud

3.2.6.1 *Definition:*

Securities and investment fraud is fraudulent conduct involving the dissemination of false information about share market members to manipulate market prices and/or attract investors.

[21] *Ibid*

[22] http://www.ftc.gov/opa/2002/01/idtheft.htm

3.2.6.2 *Current issues:*

Members of the ABA operate brokerage and financial advice services as well as banking facilities.

3.2.6.3 *Impact:*

Any fraudulent share market manipulation could adversely affect ABA members by degrading the trust in and credibility of their businesses.

3.2.6.4 *How banks are addressing*

Banks have very strict rules governing the activities of those employees, agents and associates who participate in, or can influence share (and other) market transactions. ABA members fully comply with the Australian Stock Exchange's listing rules.

3.2.7 Sales and Investment Fraud

3.2.7.1 *Definition:*

This crime includes the use of the Internet as a vehicle to solicit investments in either non-existent investment opportunities or grossly exaggerated investment opportunities. ASIC has developed a substantial amount of material dealing with such Internet investment scams[23].

Another aspect of this crime is the establishment of bogus websites that appear to be legitimate. On 9 April 2003, ASIC issued a press release which in part stated:

> *'In the past few weeks, customers of well-known institutions like the Commonwealth Bank and AMP Banking have been targeted by people using fake websites to mimic official sites', ASIC Director of Consumer Communication, Dr Michael Dunn said.*
>
> *Phoney websites and fraudulent emails can look genuine by using:*
>
> - *the names of real people;*
> - *the right logos and branding;*
> - *links to pages on the real website;*
> - *official-looking fine print; and*

[23] available from ASIC's Financial Tips and Safety Tips Website (FIDO) http://www.fido.asic.gov.au/

- *genuine pages copied to a new fake address.*

Banking and making payments over the internet can be convenient and safe so long as you take a few precautions. Use these six safety checks to protect yourself from this scam[24].

The Banks have made a concerted effort to monitor this type of activity and inform their customers of the risks involved and how to protect themselves.

ASIC has also made 6 recommendations concerning Internet banking.[25]

3.2.7.2 Current issues:

It is estimated that 67% of Australian adults accessed the Internet in the 12 months to September 2001, and that 37% of Australian households were connected to the Internet at November 2000. The ability of sales and investment fraud schemes to reach a large potential audience has expanded considerably.[26] It is also estimated that 54% of the Australian adult population owns shares, with 28% of direct shareholders stating they used no professional (broker, accountant, non-bank/bank planner or solicitor) as their source of advice in relation to investments. There would appear to be significant potential for Internet based fraudsters to take advantage of these investors.[27]

3.2.7.3 Impact:

ASIC states that there has been a significant increase in the use of the Internet to commit offences relating to investment and securities, with electronic enforcement requests growing from 8 to more than 200 within a period of two years.[28]

Being able to gauge the true extent of the number of offences that are taking place is limited by the number of reported complaints, with several studies carried out in the USA and Europe suggesting that only one third of victims of such crimes report the incidents.[29]

---

24 http://www.asic.gov.au/asic/asic_pub.nsf/byheadline/03-121+E-fraud+-+are+you+at+risk%3F?openDocument

25 ibid

26 Inman, K and Perry, D, "Investigating Internet Fraud", *ASIC*, Presented at National Investigations Symposium 7 & 8 November 2002 Sydney, 19 September 2002, p 2.

27 *Ibid,* p 3

28 *Ibid, p.4*

29 *Ibid, p 3*

3.2.7.4 How banks are addressing

Key measures undertaken by banks include:

- Prevention. Customer and merchant education; authorisation and compliance processes; Internet security measures.
- Detection. Risk management tools; exception reporting; IT security measures.
- Investigation. Specialist in-house investigation and risk management teams; liaison with law enforcement agencies.

Education is the most effective mechanism to prevent sales and investment fraud, and all stakeholders must contribute.

See Appendix A for further detail on measures undertaken.

3.2.8 Other

Other categories of financial cybercrime include fraudulent online auctions. According to the US Federal Trade Commission, this is the fastest growing and most frequently reported Internet fraud.

This crime occurs when a website is established to provide an online market between sellers and buyers. In some cases, criminals post non-existent products and are able to receive payment through a fake escrow arrangement. In other cases, there are legitimate goods on offer but the seller never receives payment because the online auction operator absconds with the payment.

3.3 Summary of current industry responses to the threat of cybercrime

3.3.1 Education

Banks conduct a wide variety of education programs for customers and merchants, aimed at improving financial literacy with respect to cybercrime. See Appendix B for a summary of the types of program in use.

3.3.2 Risk management

A recent US report on fraud prevention strategies[30] outlined key risk management strategies for fraud:

[30] Fraud Prevention Strategies for Internet Banking, April 2003, a publication of the BITS Fraud Reduction Steering Committee, www.bitsinfo.org

"In order to mitigate risk associated with online banking, financial institution policies and systemic controls should create an environment in which fraud can be prevented, detected, monitored and benchmarked against industry standards. These policies and controls should:

- *Require "reasonable efforts" to be made to ascertain the true identity of individual customers and/or the stated business purpose of each commercial enterprise with which the bank conducts business.*
- *Have a know your customer (KYC) policy that includes the following for personal account opening:*
  - *Proper identification of the customer;*
  - *Validation of the customer's residence or place of business;*
  - *Consideration of the source of funds used to open an account; and*
  - *Checking with a service bureau, if applicable, for undesirable customer behaviour such as insufficient funds or check kiting*[31].
- *Have adequate ongoing monitoring systems in place to identify suspicious transactions, such as structuring, transactions inconsistent with the nature of a customer's stated business purpose, and unusual wire activities. Various operational controls are available to mitigate fraud risk, including:*
  - *Monitoring transactions coming in and going out of deposit accounts using reports that identify a certain threshold and history of the activity over a specific time frame;*
  - *Creating reports that monitor large dollar deposits; and*
  - *Tracking ATM activity based on dollar thresholds over a certain time frame."*

As described above, Australian banks have implemented risk management systems and processes that thoroughly address each one of these principles.

[31] The use of reports from a credit reporting agency is not permissible under Australian legislation.

3.3.3 ABA Fraud Taskforce

The ABA launched the Fraud Taskforce in December 2002. In addition to the heads of fraud departments in the banks, the Taskforce also includes the commanders of the fraud squads in State and Territory police services, officers of the AFP and the High-Tech Crime Centre, and representatives of other financial services industry bodies. The Taskforce is now working on a number of major projects. Three have been publicly announced:

- The development of voluntary Industry Standards on Security and Fraud Prevention;
- An Analytical Study of Identity Documents;
- The development of a Fraud Education program for banking customers.

The development of voluntary Industry Standards on Security and Fraud Prevention will be targeted at all banking transactions, electronic and face-to-face. The standards will cover interface requirements, authentication and verification processes, and source document validation.
The Analytical Study of Identity Documents will examine the use, exchange and compilation of documents required for the validation of a bank customer's identity, particularly when opening an account. This study may lead to the Fraud Taskforce making recommendations for legislative change or investigating new processes and technology to verify a customer's identity. This study will also examine whether documents used to validate identity need any extra security measures.
The third project, Fraud Education Programme, is identifying best practice education programmes, and will create an education package for customers of financial institutions.

3.3.4 Government Collaboration

Government and industry have been working together to reduce the threat of cybercrime. An example appears in the following communiqué from Senator Ellison.

"Initiatives to Deal with Card Skimming and Identity Fraud

14 May 2003
Parliament House, Canberra
At a meeting held with representatives of peak banking and credit and debit card organisations, and law enforcement and regulatory agencies, it was agreed that:
1. THE MINISTER FOR JUSTICE AND CUSTOMS, SENATOR ELLISON WOULD HOLD BIANNUAL MINISTERIAL MEETINGS WITH FINANCIAL INSTITUTIONS TO DISCUSS FRAUD AGAINST THE FINANCE SECTOR.

2. GOVERNMENT AND INDUSTRY WELCOMED A NUMBER OF INITIATIVES WHICH HAVE ALREADY BEEN INTRODUCED BY GOVERNMENT AND INDUSTRY THAT WILL HAVE A SIGNIFICANT IMPACT ON COUNTERING CARD SKIMMING AND IDENTITY FRAUD. THESE INCLUDE:

- THE DECISION BY THE STANDING COMMITTEE OF ATTORNEYS-GENERAL TO TASK THE MODEL CRIMINAL CODE OFFICERS' COMMITTEE WITH DEVELOPING MODEL SKIMMING OFFENCES;

- THE AUSTRALASIAN POLICE MINISTERS' COUNCIL IS TO CONSIDER A NATIONAL APPROACH TO CARD SKIMMING AT ITS NEXT MEETING IN JULY 2003;

- THE AUSTRALIAN CRIME COMMISSION (ACC) IS TO UNDERTAKE AN INTELLIGENCE OPERATION INTO CARD SKIMMING;

- THE COMMONWEALTH/NSW TASK FORCE TO COMBAT ID FRAUD, CHAIRED BY THE AUSTRALIAN FEDERAL POLICE (AFP); AND

- THE AUSTRALIAN BANKERS'ASSOCIATION FRAUD TASK FORCE.

3. THE AUSTRALIAN HI-TECH CRIME CENTRE (AHTCC) WILL WORK WITH AUSTRALIAN FINANCIAL SECTOR REPRESENTATIVES AND STATE AND TERRITORY LAW ENFORCEMENT AGENCIES IN PROGRESSING WAYS TO FACILITATE MULTI-JURISDICTIONAL INVESTIGATIONS INTO SERIOUS AND COMPLEX MATTERS THAT INVOLVE IDENTITY FRAUD. THE E-CRIME COMPONENT OF THESE INVESTIGATIONS IS A HIGH PRIORITY.

4. THE AFP, ACC, ABA AND FINANCIAL SECTOR REPRESENTATIVES ARE PARTNERS IN SUPPORTING A NATIONAL APPROACH TO IMPROVED COLLECTION, ANALYSIS AND DISSEMINATION OF INTELLIGENCE ON SKIMMING AND ASSOCIATED FRAUDS. THE MEETING SUPPORTED THE DEVELOPMENT OF FURTHER INTELLIGENCE LINKS BETWEEN INDUSTRY AND LAW ENFORCEMENT ON THESE AND OTHER MATTERS OF MUTUAL INTEREST OR CONCERN."[32]

[32] 14 May 2003 - Government and industry tackle fraud against financial institutions

4. Critical Infrastructure Protection

4.1 Definition:

The Commonwealth has defined "critical infrastructure" as that infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, will significantly impact on the social or economic wellbeing or affect national security or defence. Clearly the banking sector is a vital component of the critical infrastructure. The ABA members take their collective responsibilities seriously but is must be appreciated that the banking sector is dependent upon at least two other components of the critical infrastructure, namely the electricity sector and the telecommunications sector.

4.2 Industry interdependency

The financial services sector has moved from a bricks and mortar environment to an information environment. A major disruption to electricity or the supply of telecommunication services is likely to adversely affect the supply of information for financial services.

Certain measures can to be implemented for short-term disruption in the supply of electricity (eg small fossil fuelled generators are now widely deployed for backup purposes in buildings) but these measures are not sustainable for long-term disruptions

In February 2002, a major trans-Pacific fibre optic cable off the coast of Shanghai was damaged and it required 4 to 5 days to fix the problem. This was the main cable between the USA and China, and the fault affected millions of Internet connections and was rumoured to have cost China many millions of dollars in lost transactions.[33] The Auckland power blackout in 1998, where all the main power cables supplying the inner city area failed, forcing hundreds of businesses to shut down and leaving thousands of people without electricity, is another example of industry interdependency on critical infrastructure.

4.3 Current Government response:

In November 2001, the Prime Minister announced the formation of the Business – Government Task Force on Critical Infrastructure. After a meeting in early 2002 of the task force members, the government announced in November last year, its intention to form the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). Within TISN it is proposed that there be a number of Infrastructure Assurance Advisory Groups (IAAGS) that will include owners and operators of critical infrastructure in the same sectors. It is expected that these groups will share information concerning:

- attacks or failures which have occurred within the information systems that may expose a vulnerability which could affect others in the sector;
- identification of a vulnerability not yet exploited; and

[33] Lawson, S. "Cable cut hits China hard", *IDG News Service*, ITworld.com 2/15/01

- working on "fixes" of potential problems before they become public.

A paper has been released concerning the various legal impediments to an IAAG undertaking this role. In particular, there are trade practices issues concerning sharing of information between competitors, ASIC and ASX issues about disclosure of information to the public, confidentiality issues generally, freedom of information risk and privacy requirements.
An appropriate framework needs to be worked out so that an IAAG can function within TISN.

4.4 Banking Sector approach

The ABA is working closely with the Business – Government Task Force in establishing an appropriate framework and has agreed to take a lead role in the financial sector IAAG.
A large proportion of Australia's critical infrastructure is owned privately[34]. A key component of this critical infrastructure is the banking system. The protection of this banking infrastructure has traditionally been borne by the banking sector. Banks obviously have a vested interest in not relinquishing their responsibilities, but governments also have an obligation to assist banks and other operators in the protection of the entire critical infrastructure.
The protection of Australia's critical infrastructure cannot be carried out solely by government agencies or by individual companies. The ABA agrees with the Government that:

> *"to achieve success, industry leaders and government need to work together to raise awareness of infrastructure security risks across the nation. It is also important to note that, while terrorism has assumed a higher profile in Australia's threat environment, it is not the only threat to critical infrastructure. Critical infrastructure can be damaged or destroyed by computer hackers, criminal activity, malicious damage, accidents and natural disasters. Our critical infrastructure has to be protected against all of these threats."*[35]

This can only be achieved by co-operation between all relevant. The Commonwealth Government should assist the banking industry in forging closer relations with both the electricity and telecommunications industries so that there exists a unified critical infrastructure protection platform.
In part the electricity industry and the telecommunications industries are dependent upon a stable financial sector but these industries can still meet their obligations even if there was a significant disruption to the provision of financial services, but the reverse does not hold. If either of these other critical infrastructure segments were to fail on a broad scale, the financial system would cease to function.

---

34 http://www.cript.gov.au/www/CriptHome.nsf/HeadingPagesDisplay/What+is+Critical+Infrastructure?OpenDocument

35 ibid.

5. Legal Analysis

5.1 Legislative Framework that Impacts upon Cybercrime

There is currently an extensive legislative framework deployed against cybercrime. This submission will concentrate on Commonwealth legislation but set out in Appendix E, there is a summary description of State regulatory structures.

5.1.1 Criminal Code Act 1995 (Cwth):

Division 12 of the Federal *Criminal Code*[36] concerns corporate responsibility in criminal matters. The general principles for the application of the Federal *Criminal Code* are set out in section 12.1:

12.1 General principles

(1) This Code applies to bodies corporate in the same way as it applies to individuals. It so applies with such modifications as are set out in this Part, and with such other modifications as are made necessary by the fact that criminal liability is being imposed on bodies corporate rather than individuals.

(2) A body corporate may be found guilty of any offence, including one punishable by imprisonment.

The central concept of Division 12 is that a corporation can be held criminally liable for the actions of its employees if the corporation has a corporate culture of non-compliance with Commonwealth laws.

The term "corporate culture" is defined to mean an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place.

These provisions ensure that corporate Australia must create an environment that is conducive to complying with the Commonwealth laws and that if a corporation fails to do so, it can be held criminally liable if an employee commits an offence against a Commonwealth law, including those listed below.

[36] The Criminal Code Act 1995 is generally referred to as the Federal Criminal Code.

5.1.2 Cybercrime Act 2001(Cwth)

The *Cybercrime Act* came into force on 15 December 2001. The Act covers not only unauthorised activity on Commonwealth computers[37] but also unauthorised activity of non Commonwealth computers where:

(a) the data is held on behalf of the Commonwealth; or

(b) the unauthorised activity is conducted via a telecommunications service[38].

It is also an offence if a person with knowledge causes an unauthorised impairment of electronic communication to or from a computer via a telecommunications service or the computer that is being impaired is a Commonwealth computer.

The penalty for persons who contravene these provisions is 10 years imprisonment.

In January 2001, the Standing Committee of Attorneys-General agreed to give priority to the adoption of State and Commonwealth legislation for computer offences, to cover the risk of cybercrime in all Australian jurisdictions. The committee's report, *The Damage and Computer Offences Report*, is meant to form the basis of legislation in each jurisdiction in Australia. So far, only New South Wales and Victoria have enacted similar provisions to the Commonwealth legislation. It is of fundamental importance that State Governments enact this legislation as soon as possible.

5.1.3 Privacy Act 1998 (Cwth)

The *Privacy Act 1998* was amended by the *Privacy Amendment (Private Sector) Act 2000 (Cwth)*. These amendments came into force on 21 December 2001. The principal effect of these amendments is that all corporations with a turnover in excess of $3 million dollars have to comply with the national privacy principles (NPP), which govern the collection, storage and use of personal information.

---

[37] A Commonwealth computer is any computer or computer system owned leased or operated by the Commonwealth.

[38] Section 477.2 of the CA.

NPP4, which relates to information security systems, provides that:

> *An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.*

Only New South Wales and Victoria have enacted privacy legislation complementary to that of the Commonwealth.

Banks take security of all information very seriously, including the personal information of their customers, and have expended substantial sums in ensuring that they comply with the NPPs. Banks are at the forefront of privacy compliance in Australia.

A report was prepared for the Office of the Privacy Commissioner in 2001 on business's progress towards meeting their obligations under the new privacy legislation.[39] The report was based on a survey of industry participants, and concluded that the Finance and Insurance industry sector was better prepared for and more knowledgeable about privacy law.

5.1.4 Proceeds of Crime Act 2002 (Cwth)

The principal objects of this Act are to deprive criminals of any benefit from committing crimes. This deprivation includes not only the confiscation of property derived or acquired out of the proceeds of crime, but also includes any benefits that a criminal may gain from publishing their activities through journalistic endeavours.

Under part 3-3 of the Act, an officer may give to a financial institution (a bank) a notice requiring the institution to provide information or documents:

(a) confirming whether an account is held by a specified person with the bank;

(b) confirming whether a particular person is a signatory to an account;

(c) if a person holds an account with the bank, the current balance of the account;

(d) details of transactions on such an account over a specified period of up to 6 months;

(e) details of any related accounts (including names of those who hold those accounts); and

[39] "Privacy and Business", prepared for the Office of the Federal Privacy Commissioner, Roy Morgan Research, July 2001 http://privacy.gov.au/publications/rbusiness.html

(f) details of transactions conducted by the bank on behalf of a specified person.

These provisions are very extensive and no changes are needed.

5.1.5 Financial Transactions Reporting Act 1990

This legislation has been discussed above and no further comments are necessary. The ABA submits that the powers given to AUSTRAC are extensive and no changes are needed.

5.1.6 Payment Systems Regulation Act 1998

This Act is administered by APRA and provides for the regulation of payments systems and purchase payment facilities such as:

(a) debit card facilities

(b) credit card facilities

(c) stored value card systems (smart cards)

In particular the Act covers such matters as:

(a) standards for payment systems;

(b) dispute resolution procedures; and

(c) access regimes on participants.

No changes are necessary.

5.1.7 Mutual Assistance in Business Regulation Act 1992

The *Mutual Assistance in Business Regulation Act* (MABRA) provides a regime under which ASIC, the ACCC and APRA can provide assistance to foreign regulators[40]. MABRA cannot be used to gather evidence for criminal proceedings.[41] Section 10 provides that a Federal regulator such as ASIC, APRA or the ACCC can serve a notice on a person, which could include a bank, requiring that bank to provide information, produce documents or provide evidence. It is an offence to fail to comply with such a request and

[40] See AEGC "Issues Paper : Mutual Assistance and Electronic Crime", July 2001 Commonwealth of Australia.

[41] The Mutual Assistance in Criminal Matters Act 1987 deals with assisting foreign authorities in criminal matters. This Act has more stringent procedural requirements that the MUBRA.

there is no privilege against self-incrimination, although the evidence gathered cannot be used in criminal proceedings.

Banks understand their responsibilities and will continue cooperate with any investigations, including cybercrime investigations.

5.1.8 Telecommunications Act 1997

As previously noted, the banking sector relies heavily on the telecommunications sector and although the *Telecommunications Act* (TA) does not directly affect the industry, there is one provision that is relevant to this submission. Section 313 of the Act provides that a telecommunications carrier must do its best to prevent its facilities from being used in the commission of offences against the laws of the Commonwealth or of the States and Territories. This includes cybercrime.

This provision is potentially very extensive in coverage and should be in appropriate circumstances enforced to ensure that telecommunications carriers fulfil their part in the prevention of cybercrime.

5.1.9 Telecommunications Interception Act 1979 (Cwth)

The *Telecommunications Interception Act* (TIA) establishes the offence of intercepting telecommunications without authority. The use of wireless communications has recently been developed into a new mechanism for telecommunications. The 802.11b protocol is an internationally developed protocol that will permit organisations to communicate with each other or to conduct internal communications by wireless means. It does away with a wired infrastructure, but still allows computers and voice over IP (VOIP) telephone technology to be used. Many organisations including ABA members have investigated the deployment of wireless communication technology including 802.11b technology.

There appears to be an anomaly within the TIA. Section 7 of the Act prohibits the interception of a message over a telecommunications network.

The definition of "telecommunications network" excludes "*carrying communications solely by means of radiocommunication.*" Many organisations in Australia are already moving to radiocommunication in the deployment of 802.11b systems.

As a representative of major potential users of wireless technology, the ABA is concerned about this anomaly and recommends that it should be rectified. It is noted that the *Cybercrime Act* also has a definition of

"telecommunications network" but this definition does not include the exception.

5.1.10 Australian Crime Commission Act 2002

The Australian Crime Commission (ACC) plays an important function in crime prevention, investigation and prosecution and deals with the global aspect of organised crime. Division 2 of the *Australian Crime Commission Act 2002* details the powers of an examiner to conduct proceedings, summon witnesses and take evidence in relation to any matter that the ACC is investigating. Any failure to co-operate with an investigation could result in criminal liability.

Although these extensive powers can be used against bank officers and employees, the ABA regards them as necessary and sufficient.

5.1.11 Charter of the UN Act 1945 (Cwth)

The Act is in response to Australia's international obligations as a member of the United Nations. One of the matters covered by this Act is terrorism in Australia and the ability for authorities to seize the assets of terrorists and terrorist groups. This Act provides that the Attorney-General may by notice seize any assets of any person or group in order to give effect to a Security Council decision.

These provisions are also extensive and no changes are required.

5.1.12 Banking Act 1959 (Cwth)

Under Section 11AF of the *Banking Act*, the Australian Prudential Regulatory Authority (APRA) has power to determine standards in relation to prudential matters for banks.

A failure to comply with a standard is not an offence but could lead to APRA giving a direction under Section 11CA. This section gives APRA extremely wide powers in relation to making directions, including a direction to comply with a standard or to undertake particular conduct or to terminate the employment of officers and employees. Failure by a bank to comply with a direction is an offence. Officers who fail to implement a direction are also guilty of an offence.

In September 2000, APRA issued Standard No. APS310, which is called "Audit and Related Arrangements for Prudential Reporting". Principle No. 4 reads:

> *"It is the responsibility of [a bank's] board and management to ensure that the [bank] meets prudential and statutory requirements and has management practices to limit risks to prudent levels. The risk management practices must be detailed in risk management systems descriptions which should be regularly reviewed and updated (at least annually) to take account of changing circumstances."*

As banks have a fundamental dependence on information systems, the exposure of those systems to criminal activity falls under the risk management process.

Recently APRA has recruited staff experienced in information security to add to its audit staff. The ABA has been working with APRA to ensure adequate, achievable and world standard practices are adopted to measure Australian banks' management of information risk. This is an ongoing process.

No additional regulator involvement is considered necessary at this time.

The possibility that a failure to adhere to standards could lead to a direction under Section 11CA is a major incentive to all banks to adopt stringent risk management standards. No further incentive is required.

5.2 Self regulation and co-regulation

In addition to the legislation above, there are various codes of practice that need to be considered in relation to cybercrime. The development of industry codes of practice complies with the Minister for Financial Services and Regulation's Taskforce Report on "Industry Self Regulation"[42]. This report recommended that instead of Parliament legislating on various matters, industry should establish industry codes of practice and that regulatory authorities like APRA, ACCC and ASIC should oversee compliance. In particular, it was stated by the Self Regulation Task Force that codes of conduct, if appropriately drafted, are much more cost effective for business and consumers than legislation and can be more efficient in the resolution of disputes. Many industries including the banking sector have developed or are subject to industry codes of practice. Codes that directly affect the banking sector include:

[42] http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/contents.asp

5.2.1 Code of Banking Practice

The ABA has developed with industry the Code of Banking Practice(CBP)[43] the new version of which will come into force in August 2003. This code represents a commitment by the banking sector to provide fair and world's best banking practices that will benefit all Australians.

In relation to electronic communication, the CBP refers to the Electronic Funds Transfer (EFT) Code of Conduct.

5.2.2 EFT Code of Practice

ASIC administers the EFT code of practice. The EFT code was recently updated to take into account new technologies such as the Internet transactions and smart cards[44]. ASIC has noted that[45]:

> *To the best of our knowledge all institutions offering ATM and EFTPOS transfers at the time of the monitoring period had adopted the EFT Code of conduct. Since the period under review, adoption of the revised EFT Code has also been encouraging and we now have over 220 signatories to the revised code an increase over the 199 members at the time of this monitoring report.*
>
> *Most code members reported full compliance with each of the provisions in the respective codes.*

5.2.3 Australian Payments Clearing System (APCA)

APCA is a company limited by guarantee that sets, manages, and develops procedures and standards governing payment, clearing and settlement systems in Australia. Its members are the banks, credit unions, building societies and other institutions and companies participating in APCA's five payments clearing systems. One of those payments systems is the Consumer Electronic Clearing System (CECS). CECS is the system and procedures made for:

(i) the purpose of facilitating the co-operative development by CECS members of:

---

[43] The new Code of Banking Practice will not commence until August 2003. A copy of the existing Code is set out in Appendix F.

[44] 1 April 2002 the revised EFT code into effect.

[45] see "Compliance with the Payment Systems – Codes of Practice and EFT Code of Conduct : April 2001 – March 2002" released March 2003 by ASIC.

(a) standards, policies and procedures which ensure the efficient and secure exchange of items between members; and
(b) principles relating to the settlement of the obligations incurred as a result of such exchanges; and

(ii) the exchange of financial data.

APCA publishes the Regulations for the Consumer Electronic Clearing System, which came into effect in December 2000. These regulations govern each member's participation in the CECS. In addition to the CECS Regulations, APCA has also developed the CECS Manual that details the operations procedures, specifications, checklists and guidelines that the CECS management committee has approved. The development of these documents and their compliance by CECS members further assists in the establishment of a secure and stable financial environment

5.3 Liability issues

Cybercrime in Australia is not a single stakeholder issue. Customers, banks, other industries and governments all have a vital role in managing the risks involved in conducting business via telecommunications services.

The main role for customers is in understanding what is expected of them, for example in relation to protecting their credit card information and other financial information. Governments need to facilitate this understanding by providing education programs.

There is in Australia an extensive regulatory regime for banking and cybercrime. Each of the Acts discussed above can impose severe penalties for non-compliance. There are number of regulatory authorities that have the power to issue directions to banks and failure to comply with such directions can result in criminal prosecution, with a possibility of a custodial sentence.

The ABA believes that the current regulatory framework sufficiently covers the risks arising from cybercrime and that no further regulatory or reporting burden need be imposed.

In relation to actual and potential offenders however, there may be an opportunity and a need to review the sanctions for so-called "White Collar Crimes" to ensure there is a sufficient element of deterrence.

6. Recommendations

The ABA makes the following key recommendations:

1. The Australian regulatory framework is comprehensive and far-reaching, and apart from the implementation of uniform cybercrime and privacy legislation by all States and Territories, and a review of criminal sanctions, no changes are required.

   In particular, adequate legislation exists to:
   - Make cybercrime criminal (*Cybercrime Act*, *Criminal Code*, *Privacy Act*, *Telecommunications Act*, *Telecommunications Interception Act*);
   - Report suspicious behaviour (*Financial Transactions Reporting Act*);
   - Investigate crime (*Australian Crime Commission Act*);
   - Recover proceeds (*Proceeds of Crime Act*);
   - Cross international boundaries (*Mutual Assistance in Business Regulations Act*);
   - Seize assets (*Charter of the UN Act*); and
   - Adopt prudential standards (*Banking Act*).

   In addition, the banking industry has adopted world class codes of practice.

2. There is a significant role for Government in educating the general public on their responsibilities in relation to cybercrime and on preventative measures. A programme similar to the Government's recent campaign on terrorism might be considered, the costs of which could be shared between Commonwealth and State Governments.

3. There is a significant opportunity for Government and banks to collaborate on Critical Infrastructure Protection as a defence against cybercrime, locally and internationally. This assistance should not only involve the establishment of the appropriate forums, but should also include financial assistance to all sectors of the critical infrastructure. Such assistance could include education funding and the funding of specialist research projects. Government could also consider providing special tax incentives for banks and others to cover the critical infrastructure maintenance costs, as the infrastructure benefits the entire nation.

4. Only the banks have the skills and resources necessary to manage the risks of cybercrime to the banking system. If Government were to form the view that it was in the national interest for a new cybercrime reporting or information-sharing mechanism to be established (within TISN or otherwise), the most

effective model would be an industry-managed system, with appropriate assistance from Government.

5. It is recommended that an Government/industry consultation process be established to confirm the definition and scope of cybercrime, conduct joint analysis on the issues and impacts, and collaboratively develop any new solutions required.

Appendix A: Details of Measures Adopted by Banks

Following are examples of measures used for the prevention, detection and investigation of certain financial crimes. Measures target the customer, the merchant and bank staff. Not all measures are implemented by all banks in Australia, but there is a high penetration of the tools mentioned, and widespread implementation of the listed categories of risk management systems and processes.

Credit Card Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
Customer	Maintaining Security of Card	Statement of account	Law Enforcement Agencies (LEA)
	Monitoring of account activity	Balance enquiry via ATM/Branch/ Telephone	Card Schemes
	Card security features	Ulitising the ACI Proactive Risk Manager (PRM) a neural network-based fraud detection system.	Co-ordination and liaison between LEAs
	Pro-active customer contact to reissue accounts identified as "at risk"	Database interrogation for trend based analysis	Fraud files for investigation handled by Group Investigation team who liase with Police, the schemes and other financial institutions
	Customer education through ATM messaging, statement inserts & Internet communications.	Fraud detection tools - Monitor spending patterns on customer credit cards and flag alerts when spending outside the normal pattern occurs.	Specialist investigation teams within bank
	Channels for customer to report fraud - phone, fax, email	Use of neural network technology to detect fraud which is operated on a 24x7 basis for all credit card customers	Funding for law enforcement task forces (eg. NSW Taskforce Venlo)

Credit Card Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
	Education (Statement inserts, Group website)		Covert ATM cameras to identify offenders
	Verified by Visa		
	Internal controls (eg card activation processes, registered mail etc)		
	Authorizations, Merchant Card acceptance procedures, strict account application assessment.		
	Customer awareness through statement inserts and messenging sent to all customers		
	Phone scripting in call centres outlining extent of credit card fraud		

Merchant	Education - Direct - Schemes	Merchant awareness programs	In House
	Warning bulletins	Exception reporting	Law Enforcement Agencies
	Electronic stop for blocked cards	Fraud Detection tools - monitor fraudulent merchant activity indicators such as turn-over, charge-backs received, hand-keyed transactions, refunds processed, below floor-limit transactions etc.	Card Schemes
	Fraud Flyers distributed when terminals set up	Detection systems to identify merchants who may be targeted by fraudsters or using facility to perpetrate fraud	Merchant support units
	Quarterly Newsletters containing fraud topics		Specialist investigation teams
	Seminars on the topic of fraud. Sharing of industry Best Practice/knowledge		
	Merchant newsletter		
	Clearance Limits (merchant settlement)		

	Authorizations, PIN Numbers, Merchant Card acceptance procedures, floor limits, strict merchant assessment process prior to issuing a merchant facility, telephone procedures, to assist merchants when dealing with suspicious customers		
	Merchant education on facility establishment		
Bank	Security Features	Falcon (Fair Isaac)	In House
	Education	Hunter (Experian), FraudCheck (BayCorp)	Law Enforcement Agencies
	Card scheme systems/tools	CRIS (Visa), Riskfinder (MasterCard) Authorisation Velocity Monitoring	Card Schemes
	Behavioural analysis	Behavioural analysis	Third party investigators
	Acceptance procedures	Internal exception reports	
	Systems Password protected, restricted access to staff to systems, audit trails, staff education.		

Money Laundering/Financing of Terrorism			
	Prevention/Mitigation	**Detection**	**Investigation**
Customer	Various product/service specific monitoring systems	Manual checking of DFAT lists against customer databases	In house
	DFAT Terrorist lists at branches	Loading DFAT lists into various detection/ transaction filtering systems	Dissemination of match to AFP & AUSTRAC
	Physical surveillance systems in branches	Branch staff education - suspicious banking behaviour & suspicious transaction reporting requirements	Complying with directions from AFP to assist their investigation
Merchant	Various product / service specific monitoring systems	Fraud detection tool (Eagle) can pick up suspicious transactions indicative of merchant money laundering activity	In house
	DFAT Terrorist lists at branches		Dissemination of match to AFP & AUSTRAC
			Complying with directions from AFP to assist their investigation
Bank	Minimum standards on Anti-Money Laundering	Ongoing staff training	In house
	Money-laundering detection tools	Whistleblowers hotline	Dissemination of match to AFP & AUSTRAC
	AML risk management principles considered as part of developing new products & services	Hunter (includes OFAC lists)	Complying with directions from AFP to assist their investigation
	Behavioural analysis tools	Exception reporting	

Money Laundering/Financing of Terrorism			
	Prevention/Mitigation	**Detection**	**Investigation**
	Investigation of suspicious transactions	Reported on suspicious transaction report	
Payment/ Financial System	Accounts vetted for names of suspected terrorists	Exception reporting	In house
	Payment searching function	IMT filtering software	Forwarding of match to AFP & AUSTRAC
	Prudential limits (including cumulative)	Hotscan (Logica CMG) - scans and matches swift payments against proscribed lists as gazetted by various governments - DFAT, OFAC	AFP
	Segmented risk (eg high risk billers/payers)		Complying with directions from AFP to assist their investigation
			Investigation includes AFP assistance prior to freezing of assets

Debit Card Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
Customer	Security of Card & PIN	Account Statement	Law Enforcement Agencies
	Monitoring of account activity	Balance of Account Enquiry via Branch/ ATM/Telephone Enquiry	Card Schemes
	Education & Awareness	Database interrogation to identify fraud cases	External investigation resources and police liaison
	Security features on card	Hunter	Specialist investigation team, in house
	Debit Card Terms & Conditions governing the usage of cards		
	Transaction limits		
Merchant	Validation of card number with lost/stolen cards database	Eagle	Fraud files for investigation handled by in-house investigation teams who liase with Police, the schemes and other financial institutions
	Authorizations, PIN Numbers, Merchant Card acceptance procedures, floor limits, strict merchant assessment process prior to issuing a merchant facility, telephone procedures to assist merchant when dealing with suspicious customers	Merchant Awareness	Law Enforcement Agencies

Debit Card Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
	Electronic stop on blocked accounts	Exception reporting	Card Schemes
	Education and awareness of fraudulently prepared cards		
Bank	Stop Accounts & Block cards	In House monitoring	In House
	Capture of card at ATM	Overdrawn account identification	Law Enforcement Agencies
	Education	Surveillance cameras at ATMs	Card schemes
	Review of fraudulently identified transactions	Database interrogation to determine common points of purchase	Review by internal investigations units
	Transaction limits	Hunter	Internal checklists and regular branch reviews by Risk Management
	Acceptance processes	Exception reporting	
		100 points check	
		Controls over identification of customers at time of changing PINs	

Identity Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
Customer	100 point check	FraudCheck / VeriCheck	Internal checklists and regular branch reviews by Risk Management
	Staff Training	NSW & Victorian Birth Certificates verified online	Specialist investigation teams
	Monitoring of account activity	Customer reports	
	Identification of customers	Hunter	
	PINs	Fraudcheck	
	Transaction Card Limits	On line resources (CITEC, BDM etc)	
	Advice to customers on what to do if identity compromised	100 point check	
		Controls over identification of customers at time of changing PINs	
Merchant	100 point check	FraudCheck/ VeriCheck	In House
	Education	Cheque fraud detection system for cheque conversion - indicative of ID Fraud	
Bank	Due dilligence checks on new and existing customers	Whistleblowers hotline for internal fraud	Inform Collections/Network Operations
	Use of Hunter to match fraudulent identities	Use of Hunter to detect fradulent identities	Inform police if involves a syndicate

Identity Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
	Merchant approval teams – Baycorp searches	Electronic white pages	In-house Fraud and Risk Management
	Acceptance processes	Vericheck/Fraudcheck	Business Unit Fraud and/or Risk Team i.e. Mortgages etc
	Participation in Industry Forums	On line resources (CITEC, BDM etc)	
	Cross search against external database		

Sales and Investment Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
Customer	Confirm introducer is properly authorised - sight proper authority etc	Fund Statements	In house
	Approval of Investment plan		Law Enforcement Agencies
	Secure internet site (securities trading)		ASIC
	User ID and password access to Internet Banking	Compromise notified by customer	Reference to activity log to determine fraudulent access or repeated failed attempt to access
	Use of virus prevention software and firewalls	Trojan or spyware virus intrusion attempts blocked.	
Merchant	Broker training/auditing	Hunter/Fraudcheck/exception reporting	
	Merchant training/auditing		
Bank	Statutory Licencing	Customer advice	Law Enforcement Agencies
	Internal accreditation process	Real time rule based alerting based on known fraud trends	ASIC
	In house audit/compliance processes; settlement policy	Provision of tools and functions for customers to use to further protect against fraudulent access.	Immediate actioning by fraud operators to confirm or cancel transactions.
	Payment & receipt policy	Monthly reporting and regular review by Risk Management	Risk, Compliance and Audit department
	ASX rules	Product risk teams	Specialist investigation teams

Sales and Investment Fraud			
	Prevention/Mitigation	**Detection**	**Investigation**
	Pre-screening of employees in sales force roles (criminal history, reference checks)	Percentage checking of all lending files for validity, accuracy with bank policies and compliance with credit code requirements	
	Monitoring of all payment transactions via 3rd party provider (PRM)		
	Development of new security features within Internet Banking (Password lock)		
	Ongoing customer education regarding the protection of information		
	Exception reporting to identify and scrutinise high sales performers		
	Policy guidelines		
	Regular auditing of sales staff files		

Appendix B: Examples of Education Programs Relating to Cybercrime

Education and Financial Literacy		
	Customer	**Merchant**
Advertising	Statement inserts	Statement inserts
	Print media	Verbal training for operators calling merchants
	Email	Email merchants with fraud information
	ABA notifications and Press releases regarding the increased security relating to the latest upgrade to Internet Banking	Merchant newsletters and brochures
	Internet Banking banner messages relating to security and fraudulent scams.	Fraud bulletins
	Statement messenging	
Conditions of use and other documents of this nature	Conditions of use documentation, providing clear guidelines on responsibilities for loss, and circumstances where customer liable	Conditions of use documenation provide clear guidelines of responsibilities for loss and circumstances where customer liable
	Statement inserts	Statement inserts
	Printed Terms & Conditions for cards, accounts	Scheme literature (regular & specific)
	Electronic Terms & Conditions on Internet sites	
	Terms and Conditions brochures and Product information brochures contain messages relating to security of PIN and Passwords. This covers all electronic transaction mediums.	Merchant Agreement and user guide and installation verbal training

Education and Financial Literacy		
	Customer	**Merchant**
	Terms and conditions are available for all products and services. These have now been standardised for compliance with FSRA legislation.	Fraud information on Internet
		Terms and conditions for all products and services.
Internet	Tips on Internet banking site	Website describing all major fraud types and tips for prevention
	Linkages to anti-virus vendors and providers of firewall protection	
	Fraud prevention hints/tips for various products	
	Email messages sent to all Internet Banking customers warning of potential scams or fraudulent activity.	
	Websites describe major fraud types and tips for prevention	
	Conditions of use for all products and security and privacy statements for the website are available online.	
Marketing Collateral	Newsletters for products including Credit Cards, Investments and Home loans to educate customers about products and the market place.	Newsletter for merchants and for Small Businesses advising about products that are available and industry issues.
	Branch advertising material	
Other	ATM warning signs	Conduct of seminars for business customers to support understanding of fraud related risks and what they can do to avoid

Education and Financial Literacy		
	Customer	**Merchant**
	Branch warning signage	Broker fraud detection seminars
	Staff training	One on one training for new merchants

Appendix C: Theft of Information and Telecommunications Services

Nevada Legislation

Sec. 33. NRS 205.506 is hereby amended to read as follows:

205.506 1. It is unlawful for a person knowingly and with the intent to avoid payment in full for the service obtained to:

(a) Obtain or attempt to obtain an information service from a provider by deception, use of an illegal device or other fraudulent means. The requisite intent may be inferred from the presence on the property or in the possession of the person of a device, not authorized by the provider, the major purpose of which is to permit or facilitate use of an information service without payment. The inference is rebutted if the person shows that he purchased the device for a legitimate purpose.

(b) Give to another person technical assistance or instruction in obtaining an information service without full payment to a provider.

(c) Maintain an ability to connect, by physical, electronic or other means, with facilities, components or devices used in an information service for the purpose of obtaining the information service without payment of all lawful compensation to the provider.

(d) Make or maintain a modification of a device installed with the authorization of a provider to obtain any service that the person is not authorized by the provider to obtain. The requisite intent may be inferred from proof that the standard procedure of the provider is to place labels on its devices warning that modifying the device is a violation of law and that the device has been modified without the permission of the provider.

(e) Possess, manufacture, deliver, offer to deliver or advertise, without permission from the provider, a device or a kit for a device designed to:

(1) Receive from the provider a service offered for sale by the provider, whether or not the service is encoded or otherwise made unintelligible; or

(2) Perform or facilitate an act prohibited by paragraphs (a) to (d), inclusive.

Intent to violate this paragraph for commercial advantage or financial gain may be inferred if the circumstances, including, without limitation, quantity or volume, indicate possession for resale.

(f) Manufacture, import, distribute, advertise, sell, lease, or offer to sell or lease a device or a plan or kit for a device designed to receive an information service offered for sale by a provider, whether or not the service is encoded or otherwise made unintelligible, without full payment. The requisite intent may be inferred from proof that the person has sold, leased or offered to sell or lease

any such device, plan or kit and stated or implied to the buyer or lessee that it will enable him to obtain an information service without charge.

Appendix D: Card Skimming

The following is part of the text of a white paper published by the Hypercom Corporation. The ABA makes no warranties as to the accuracy of the material presented:[46]

Payment Card Skimming
Combatting Fraud in an Increasingly Vulnerable Global Marketplace

The Problem

Credit card skimming is a much bigger problem than we thought. Skimming is growing rapidly and is becoming very sophisticated. Skimming is victimizing consumers, causing havoc with merchants, and costing the industry hundreds of millions of dollars every year. It has the potential for damaging the relationships that form the very foundations of the credit payment industry. The entire industry has a stake in fighting skimming, especially at the point of sale, where until now little has been done.

Skimming is the fraudulent act of reading and storing the information encoded on the magnetic stripe of a debit or credit card through either an illegal miniature handheld card reader known as a "skimmer," or a skimmer bug implanted in a legitimate payment terminal. Once obtained, that information can be re-encoded onto any other card with a magnetic stripe, instantly transforming a blank card into a machine-readable debit or credit card identical to that of the cardholder whose card was "skimmed." To make matters worse, today illegal websites are being used to sell and distribute skimmed credit card data.

Skimming takes advantage of the fact that the digital content of a magnetic stripe card can be copied with perfection. There is essentially no difference between a copy and the original. The fact is that the magnetic stripe was simply not designed to withstand attacks that use the sophisticated technologies available today.

Skimming Becomes a Dangerous Global Epidemic

Skimming is rapidly growing in virtually every major city in the United States (US), United Kingdom (UK), Europe, Canada, and Latin America. It is especially rampant in Asia. It is estimated that the average skimmed credit card will generate some $2,000 in fraudulent charges before being detected and stopped. According to The Nilson Report, skimming now ranks behind only lost and stolen credit cards as a contributor to fraud losses.

Annual losses caused by skimming were reported to be over $110 million in the United States alone. "Skimming is the biggest problem in bank fraud today," says Gregory Regan, head of the US Secret Service financial-crimes division. "It's the bank robbery of the future. It's technically simple, point-and-click technology. And the equipment is cheap. If you skim 15 or 20 accounts, you can generate $50,000 to $60,000 worth of fraud, and nobody is going to know about it until the victims get their bills, 30 to 60 days after the crime. So the odds of getting caught are reduced."

Last year, the skimming racket cost UK banks almost £100 million. "The amount of money lost through credit card skimming has doubled to £250,000 per working day in

[46] http://www.hypercom.com/_Documents/_Whitepapers/Skimming.pdf

the last year," reports ITN's Personal Finance Editor, Louise Noel. Counterfeit card fraud rose by a staggering 104% in the UK, mainly because of the large number of skimming cases.

All across Asia, credit-card skimming fraud is on the rise. The favored victims are Japanese. Credit-card fraud involving Japanese has risen 45% in the past three years, while thefts in which fake cards are used has increased eightfold. Gangs from China and Malaysia target Japanese because their cards often come with high credit limits, and Japanese laws against counterfeiting are loose. "Japan is a good country for these criminals because the economy is so big, and the laws are so lax," says Akira Arakawa, security and risk manager at MasterCard in Tokyo.

Skimming theft rings are having a major impact on credit card usage at the point of sale in Asia. In fact, many Asian acquirers now require merchants to provide a security deposit of US$25,000 to cover the fines they sustain from skimming that occur in their base of merchants. This is upsetting the relationship between merchants and acquirers, as well as the relationship between the associations, issuers and the acquirers. In some cases, skimming has led to merchants declining to accept certain card brands. In other cases, it has resulted in merchants declining to accept cards altogether.

In some countries, skimming is so out of control that US travelers are being instructed by their travel associations to withdraw cash from a branch bank ATM and use the cash for purchases at merchant locations. Malaysia, Hong Kong, Belarus, Colombia, Egypt, Lithuania, Macedonia, Nigeria, Pakistan, Romania, Russia, and Venezuela are recognized high-risk countries for travelers making credit card purchases. One traveler recently reported, "back in January and February, my credit card was used to buy more than $2,700 worth of goods from a shop in southern Thailand, about $100 of goods at Sunway Plaza in Kuala Lumpur, a seafood lunch in Hong Kong, almost $1000 in clothes, also in Hong Kong, and even a $10 coffee in Malacca in Malaysia. All up, my card was used for a shopping spree of almost $7000 across Malaysia, Thailand, and Hong Kong. But I wasn't in any of these places at the time - I was in France."

How Does Skimming Work?

There are generally four places where confidential credit card information can become compromised:

- At an ATM
- At the merchant location itself
- During the transmission process used for authorization purposes
- At the point of storage.

Skimming at an Automated Teller Machine (ATM)

Card skimming was first seen at ATMs. Criminals adopted a variety of techniques to capture magnetic stripe information and customer PIN numbers. One form of fraud involved thieves removing an existing ATM and replacing it with a fake one just before the beginning of a busy weekend when a large number of cash withdrawals were anticipated. On the following Monday morning, the criminals returned and retrieved their fake ATM. The fake ATM hadn't dispensed any cash all weekend, but it did capture lots of valid card account numbers.

The second popular skimming method was the inserting of an unauthorized card reader inside the jaws of the ATM's real card reader. This prevented the machine from working but did capture lots of valid account numbers. Criminals would later retrieve the fake reader and email valid card numbers to card production plants located in the Far East or in Central/Eastern Europe.

Skimming by Clerks at the Merchant Locations

The most common form of skimming involves the use of miniature, pager size, and card readers. The skimming device is kept near the legitimate POS device in a store, or a miniature version is carried in the pocket of a waiter/waitress in a restaurant. The card is then swiped through the legitimate machine for purchase approval of the authorized transaction, and it is also run through the skimmer for the purpose of stealing the magnetic stripe information. The skimmer is used to collect the data from the magnetic stripe of up to one hundred cards. The skimmer is then plugged into a laptop. The laptop uploads the credit card numbers and the data is e-mailed or file transferred to a factory where cards are produced overnight. The next morning, cards are delivered via air transport to locations all over the globe. The cardholder is unaware that anything is wrong.

Fraud detection software now exists that can detect this type of fraud by analyzing unusual card usage patterns. These software packages, operated by the international payment associations and large bank acquirers, use artificial intelligence logic to locate Common Points of Purchase (CPP) where most skimming originates. The software is sophisticated enough to detect fraud patterns even when the criminals delay for sometimes months using copies of the original card numbers stolen. Although the fraud can be detected through analysis, the criminals are often more difficult to apprehend as skimming occurs in environments with heavy employee turnover. Criminal organizations engaged in skimming commonly bribe employees at gas stations and restaurants to do the dirty work. "They blackmail workers who are in the host country illegally to do it," says Paul Lucraft, deputy general manager for Europay International, "because these people are afraid they'll lose their jobs and be deported."

Skimming during the data capture and transmission process

A more sinister type of skimming is now emerging. This involves implanting sophisticated skimmer bugs into card payment terminals. Business Week's Ken Belson reported recently that "counterfeiters in Japan and Taiwan have taken number skimming to a new level by putting chips in machines at restaurants and other stores used to authorize credit transactions.

Criminals break into retail stores at night, swap out the POS terminal for a similar looking model, but one which has had extra wires and components added internally. This extra circuitry does not stop the machine from working, but all card numbers are now being recorded and stored in this additional chip. The criminals return a week later, attach the POS to a PC and send all the stolen card numbers to a card production facility overseas.

According to Card Alert Services, Inc, POS skimmers have become increasingly more difficult to detect.

Using a skimming bug can net a thief hundreds of card numbers in a relatively short period of time. What's even worse, Visa executives report, is that skimming is now spreading to all types of retailers from its traditional base of restaurant and convenience store.

According to George Wallner, Hypercom's Chief Strategist, "Until now, the card associations had an effective weapon to combat skimming. By using sophisticated

software they could identify the juxtaposition common to skimmed cards and thus the merchants where high levels of skimming originated. The associations could then assess fines against those merchants (and their acquirers) or withdraw their card accepting privileges. But with skimmers in terminals, skimming has jumped from the relatively concentrated high volume restaurant and gas station locations, into general retail. With this, the pattern is becoming too broad to track easily. There is no longer an easily identified CPP. As a result, the industry's most effective anti-skimming tool - AI software -- has become less effective."

ABA Consumer Tips[47]

As a banking customer, there are steps you can take to safeguard yourself and your money. We're offering you some tips on protecting your money, credit, debit and ATM cards against fraud and misuse.

1. Your Personal Identification Number (PIN) is a number that is entered by a customer when using an ATM or EFTPOS terminal and it gives you access to your account. It is in effect your electronic signature and you are the only person who should know it. No one from a financial institution, the police or a retailer should ask for your PIN number. If anyone does ask for it – do not reveal it.

2. If you are using your credit card to pay for goods and service, a signature will be required. Your will need to punch in your PIN number on the EFTPOS machine if you want to use funds in your account to pay for a good or service.

3. Conducting a transaction at an ATM or an EFTPOS terminal requires your access card and your PIN number. Do not write it down – memorise it if you can. If you do need to keep a record, keep the PIN number in a safe place, not in your wallet.

4. When a bank issues an access card, it will give you a PIN number. You have the option of changing the PIN to a number or word that you have personally chosen. When selecting a PIN always avoid the obvious – your name, telephone number, date of birth, or address.

5. Your access card is the key to your accounts. It is for your use only. Keep it in a safe place, don't lend it to another person and do not tell anyone your PIN number.

6. Immediately notify the bank if you have lost your card or if your PIN record is lost or stolen, or if you suspect that unauthorised transactions have been made on your account. This will enable your bank to put a stop on your card straight away, so no one else will be able to use it. Banks offer telephone numbers to

[47] http://www.bankers.asn.au/

call when reporting lost or stolen cards or PINs, keep these numbers handy, or program them into your mobile phone.

7. Conduct your electronic transactions where your feel most secure. If you are uncomfortable using a terminal at any time, there are always alternatives – such as at a supermarket while buying groceries.

8. To ensure privacy when conducting a transaction at a terminal, use your body as a shield to prevent others seeing you enter your PIN number.

9. Once you've completed your ATM transaction, put your money away immediately and leave. Count your money as soon as it is safely possible to do so.

10. If you simply want to check your account balance or transfer funds between accounts, phone banking or Internet can be used instead of an ATM.

11. After completing a transaction, remember to take your card and if requested, the receipt of your transaction record.

12. When using your card to pay for purchases, keep it in sight and ensure all receipts are obtained so you can check your statement. Keep all your credit card receipts in a safe place because they do carry your credit card number.

Appendix E: FATF Recommendations

Introduction

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering -- the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities.

The FATF currently consists of 29 countries [1] and two international organisations [2]. Its membership includes the major financial centre countries of Europe, North and South America, and Asia. It is a multi-disciplinary body - as is essential in dealing with money laundering - bringing together the policy-making power of legal, financial and law enforcement experts.

This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the forty FATF Recommendations -- the measures that the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the Forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem. [3]

These Forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international cooperation.

It was recognised from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.

FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the Forty Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.

These measures are essential for the creation of an effective anti-money laundering framework.

Footnotes:

[1] Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty-nine FATF member countries and governments are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States.

[2] The two international organisations are: the European Commission and the Gulf Co-operation Council.
[3] During the period 1990 to 1995, the FATF also elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations. The FATF adopted a new Interpretative Note to Recommendation 15 on 2 July 1999.

General Framework of the Recommendations

Recommendation 1
Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention)

Recommendation 2
Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

Recommendation 3
An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

Role of National Legal systems in Combating Money Laundering

Scope of the Criminal Offence of Money Laundering

Recommendation 4
Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalise money laundering as set forth in the Vienna Convention. Each country should extend the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences.

Recommendation 5
As provided in the Vienna Convention, the offence of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

Recommendation 6
Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

Provisional Measures and Confiscation

Recommendation 7
Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offence, or property of corresponding value, without prejudicing the rights of bona fide third parties.
Such measures should include the authority to: 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.
In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void

contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

Role of the Financial System in Combating Money Laundering

Recommendation 8

Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively.

Recommendation 9

The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

Customer Identification and Record-keeping Rules

Recommendation 10

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

i. to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

ii. to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

Recommendation 11

Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

Recommendation 12

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

Recommendation 13

Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

Recommendation 14

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Recommendation 15

If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities

Recommendation 16

Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Recommendation 17

Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

Recommendation 18

Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

Recommendation 19

Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

i. the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

ii. an ongoing employee training programme;

iii. an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

Recommendation 20

Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

Recommendation 21

Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Other Measures to Avoid Money Laundering

Recommendation 22

Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

Recommendation 23

Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

Recommendation 24

Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers

Recommendation 25

Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

Implementation and Role of Regulatory and Other Administrative Authorities

Recommendation 26

The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

Recommendation 27

Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

Recommendation 28

The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

Recommendation 29

The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

Strengthening of International Co-operation

Administrative Co-operation

Exchange of general information

Recommendation 30

National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

Recommendation 31

International competent authorities, perhaps Interpol and the World Customs Organisation, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

Exchange of information relating to suspicious transactions

Recommendation 32

Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Other Forms of Co-operation

Basis and means for co-operation in confiscation, mutual assistance and extradition

Recommendation 33

Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions - i.e. different standards concerning the intentional element of the infraction - do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

Recommendation 34

International co-operation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

Recommendation 35

Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Focus of improved mutual assistance on money laundering issues

Recommendation 36

Co-operative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.

Recommendation 37

There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

Recommendation 38

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

Recommendation 39

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

Recommendation 40

Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offence or related offences. With respect to its national legal system, each country should recognise money laundering as an extraditable offence. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests

or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Annex to Recommendation 9: List of Financial Activities undertaken by business or professions which are not financial institutions

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.[1]
3. Financial leasing.
4. Money transmission services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts...)
6. Financial guarantees and commitments.
7. Trading for account of customers (spot, forward, swaps, futures, options...) in:
    a. money market instruments (cheques, bills, CDs, etc.) ;
    b. foreign exchange;
    c. exchange, interest rate and index instruments;
    d. transferable securities;
    e. commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of clients.
11. Life insurance and other investment related insurance.
12. Money changing.

Footnote:

[1] Including inter alia

- consumer credit
- mortgage credit
- factoring, with or without recourse
- finance of commercial transactions (including forfeiting)

Appendix F: State Legislation

State cybercrime offences:

Australian Capital Territory

- Theft (s.9 *Crimes Act 1900*)
- Obtaining a financial advantage by deception (s.104(1) *Crimes Act 1900*)
- Making a false instrument (s.135C(1) *Crimes Act 1900*)
- Using a false instrument (s.135C(2) Crimes Act 1900)
- Unlawful access to date in computer (s. 135 J *Crimes Act 1900*)
- Damaging data in computers (s.135K *Crimes Act 1900)*
- Dishonest use of computers (s. 135L *Crimes Act 1900*)

New South Wales

- Fraudulent misappropriation (s.178A *Crimes Act 1900*)
- Obtaining money etc by deception (s.178BA *Crimes Act 1900*)
- Obtaining money by false or misleading statements (s.178BB *Crimes Act 1900*)
- Obtaining credit by fraud (s.178C *Crimes Act 1900*)
- False pretences (s.179 *Crimes Act 1900*)
- Fraudulent personation (s.184 *Crimes Act 1900*)
- Forging and uttering (s.250 *Crimes Act 1900*)
- Unauthorised access, modification or impairment with intent to commit serious indictable offence (s. 308C *Crimes Act 1900*)
- Unauthorised modification of data with intent to cause impairment (s. 308D *Crimes Act 1900*)
- Unauthorised impairment of electronic communication (s. 308E *Crimes Act 1900*)
- Possession of data with intent to commit serious computer offence (s. 308F *Crimes Act 1900*)
- Producing, supplying or obtaining data with intent to commit serious computer offence (s. 308G *Crimes Act 1900*)

- Unauthorised access to or modification of restricted data held in computer (summary offence) (s. 308H *Crimes Act 1900*)
- Unauthorised impairment of data held in computer disk, credit card or other device (summary offence) (s. 308I *Crimes Act 1900*)

Northern Territory

- Stealing (s.210 *Criminal Code*)
- Criminal deception (s.227 *Criminal Code*)
- Unlawfully altering data processing material with fraudulent intent (s.476(1) *Criminal Code*)
- Possession of child pornography and certain indecent articles (s. 125B *Criminal Code*)
- Unlawfully obtaining confidential information (s. 222 *Criminal Code*)
- Unlawful access to data (s. 276B *Criminal Code*)
- Unlawful modification of data (s. 276C *Criminal Code*)
- Unlawful impairment of electronic communication (276D *Criminal Code*)
- Unlawful appropriation of access time (s. 276E *Criminal Code*)

Queensland

- Stealing (s.398 *Criminal Code*)
- Fraud (s.408C(1) *Criminal Code*)
- Misappropriation (s.408C *Criminal Code*)
- Computer hacking and misuse (408D *Criminal Code*)
- False pretences (s.427(1) *Criminal Code*)
- Falsifying records (s.441(d) *Criminal Code*)
- Producing false records (s.441(e) *Criminal Code*)
- Uttering (s.489 *Criminal Code*)

South Australia

- Fraudulent conversion (s.184 *Criminal Law Consolidation Act 1935*)
- False pretences (s.195 *Criminal Law Consolidation Act 1935*)

Tasmania

- Stealing (s.229(1)(b) and 234 *Criminal Code Act 1924*)
- Dishonestly acquiring a financial advantage (s.252A(1) *Criminal Code Act 1924*)
- Inserting false information on data (s.257E *Criminal Code Act 1924*)
- Attempting to dishonestly acquire a financial advantage (s.299 *Criminal Code 1924*)

Victoria

- Obtaining property by deception (s.81(1) *Crimes Act 1958*)
- Obtaining financial advantage by deception (s.82 *Crimes Act 1958*)
- False accounting (s. 83 *Crimes Act 1958*)
- Falsification of Documents (s.83A *Crimes Act 1958*)

Western Australia

- Stealing (s.378 *Criminal Code*)
- Stealing as a servant (s.378(7) *Criminal Code*)
- Fraud (s.409(1) *Criminal Code*)
- Unlawful operation of a computer system (s. 440A *Criminal Code*)
- Forging (s.473(1)(a) *Criminal Code*)
- Uttering (s.473(1)(b) *Criminal Code*)
- Preparation for Forgery (s.474(1) *Criminal Code*)
- Attempted Fraud (s.552 *Criminal Code*)
- Conspiracy to commit fraud (s.558(1) *Criminal Code*)

Appendix G: Code of Banking Practice 1993[48]

PREAMBLE

The Code of Banking Practice (the Code) seeks to foster good relations between Banks and their Customers (as defined below) and to promote good banking practice by formalising standards of disclosure and conduct which Banks that adopt the Code agree to observe when dealing with their Customers.

Objectives

The Code is intended to -

(i) describe standards of good practice and service;
(ii) promote disclosure of information relevant and useful to Customers;
(iii) promote informed and effective relationships between Banks and Customers; and
(iv) require Banks to have procedures for resolution of disputes between Banks and Customers.

Principles

These objectives are to be achieved -

(i) having regard to the paramount requirement of Banks to act in accordance with prudential standards necessary to preserve the stability and integrity of the Australian banking system;
(ii) consistently with the current law and so as to preserve certainty of contract between a Bank and its Customer; and
(iii) so as to allow for flexibility in products and services and in competitive pricing.

Monitoring

The Australian Payments System Council may obtain from the Reserve Bank of Australia consolidated information based on reports and information provided by the Banks so that the Australian Payments System Council may provide reports to the Treasurer of the Commonwealth on compliance with the Code and its general operation.

The Reserve Bank of Australia will receive each year from each of the Banks:-

(i) a report on the operation of the Code; and
(ii) information concerning the number of disputes referred to in sections 20.3 and 20.4 of the Code, according to their categories and how each of these categories of disputes has been handled.

The information to be provided by the Banks to the Reserve Bank of Australia will be determined by the Reserve Bank of Australia with the Banks. Before such determination, the Reserve Bank of Australia will consult with the Australian Payments System Council.

Review

The Code shall be reviewed at least every three years in accordance with the Objectives and the Principles set out in this Preamble and having regard to the views of interested parties.

Staff Training

A Bank shall endeavour to ensure that its staff are aware of the provisions of this Code relevant to their duties and of the procedures for handling disputes with Customers of the Bank.

---

[48] A new version of the Code comes into effect in August 2003

THE CODE

This Code (published on 3 November 1993) is in three parts:

(i) Part A - Disclosures. This part describes the information which a Bank will provide to a Customer in respect of the Banking Services which the Bank offers to the Customer.

(ii) Part B - Principles of Conduct. This part describes certain principles of conduct which a Bank will follow in dealing with its Customers.

(iii) Part C - Resolution of Disputes. This part requires Banks to have dispute handling procedures.

1.0 DEFINITIONS AND APPLICATION

1.1 In this Code and the Preamble:

"Account" includes, amongst others, a cheque account or an account that can be accessed by a cheque.

"Bank" means a corporation authorised by law to carry on the general business of banking in Australia that has adopted this Code.

"Banking Service" means a deposit, loan or other banking facility provided by a Bank to a Customer, but does not include a service in relation to a bill of exchange, a variation of a term or condition of a facility or a debt to a Bank that arises as a result of a withdrawal of more than the amount by which an Account is in credit without the approval of the Bank.

"Customer" means an individual, when that individual, whether alone or jointly with another individual, acquires a Banking Service which is wholly and exclusively for his or her private or domestic use, but in any event does not include an individual who makes a written statement to the Bank, in relation to a Banking Service, that the Banking Service will not be acquired wholly and exclusively for that use.

"Related Entity" has the meaning set out in Section 9 of the Corporations Law.

"Standard Fees and Charges" means fees and charges normally charged by a Bank to its Customers in respect of a Banking Service at a particular time.

"Terms and Conditions" means those terms and conditions specifically applied by a Bank to a Banking Service but does not include any other terms and conditions that may apply by operation of law.

1.2 This Code is to be read subject to any Commonwealth, State or Territory legislation.

1.3 From the date on which a bank publicly announces that it adopts this Code:

(a) that Bank will be bound by this Code in respect of any Banking Service that Bank commences to provide to a Customer; and

(b) that Bank will be bound by this Code other than sections 2.1, 2.2, 2.3, 7.1, 11.2 and 17.1 to 17.7 inclusive in respect of any Banking Service it is then providing to any individual who would have been a Customer if this Code had applied at the time that individual first acquired that service.

1.4 To the extent of any inconsistency, this Code is to be read subject to the Electronic Funds Transfer Code of Conduct, which governs transactions on an account initiated through an electronic terminal by the combined use of a card and a personal identification number.

PART A: DISCLOSURES

2.0 DISCLOSURE: TERMS AND CONDITIONS

2.1 A Bank shall provide to a Customer in writing any Terms and Conditions applying to an ongoing Banking Service provided by the Bank to the Customer. Those Terms and Conditions shall:

(i) be distinguishable from marketing or promotional material;
(ii) be in English and any other language the Bank considers appropriate;
(iii) be consistent with this Code;
(iv) be clearly expressed;
(v) be provided at the time of or before the contract for the Banking Service is made except where it is impracticable to do so, in which case the Terms and Conditions shall be provided as soon as practicable after the provision of the Banking Service; and
(vi) draw attention to the availability of the general descriptive information referred to in sections 6.1 and 6.2.

2.2 Any written Terms and Conditions referred to in section 2.1 shall include a statement to the effect that the relevant provisions of this Code apply to the Banking Service but need not set out those provisions.

2.3 A Bank shall include (where relevant) the following in its Terms and Conditions applying to a Banking Service:

(i) the nature of all Standard Fees and Charges that then apply;
(ii) the method by which interest, if any, is calculated and the frequency with which it will be credited or debited;
(iii) the manner in which the Customer will be notified of changes to the Terms and Conditions and changes to interest rates, fees and charges;
(iv) if appropriate, the fact that more than one interest rate may apply;
(v) any minimum balance requirement or restriction on depositing money in, or withdrawing money from, an Account;
(vi) in respect of term deposits:
- the manner in which payment of interest and principal will be made;
- the manner in which funds may be dealt with at maturity; and
- the nature of any charge or variation to an interest rate resulting from a withdrawal in advance of maturity;

(vii) in respect of a loan to the Customer, the repayment details;
(viii) the frequency with which statements of Account will be provided;
(ix) a statement that information on current interest rates and fees and charges is available on request; and
(x) how a Customer or a Bank may alter or stop a payment service.

3.0 DISCLOSURE: COST OF CREDIT

3.1 A Bank shall make available to a Customer, a prospective Customer or an appropriate external agency the interest rates and Standard Fees and Charges applicable to a Banking Service offered by the Bank, for use in the preparation of a comparison rate.

4.0 DISCLOSURE: FEES AND CHARGES

4.1 A Bank shall, before or at the time of providing a particular Banking Service to a Customer for the first time or otherwise on request by a Customer, make available to the Customer a schedule containing the Standard Fees and Charges which currently apply to the Banking Service.

5.0 DISCLOSURE: PAYMENTS SERVICES

5.1 Where a Bank provides a Customer with a direct debit or credit payment service, an automatic payment service or access to an account by means of instruction via telephone or personal computer, the Bank shall make available to the Customer details of any bank fees or charges applying to the service.

6.0 DISCLOSURE: OPERATION OF ACCOUNTS

6.1 A Bank shall provide to a Customer or prospective Customer for a Banking Service upon request general descriptive information concerning Banking Services, including where appropriate:

(i) Account opening procedures;
(ii) the Bank's obligations regarding confidentiality of information relating to the Customer and the Customer's right to instruct a Bank in accordance with section 12.2(b) not to disclose information to a Related Entity of the Bank and the means by which that instruction can be given, such as by marking a box in an application form;
(iii) complaint handling procedures;
(iv) the Bank's right to combine Accounts;
(v) bank cheques;
(vi) the advisability of a Customer informing the Bank promptly when the Customer is in financial difficulty; and
(vii) the advisability of a Customer reading the Terms and Conditions applying to the Banking Service.

6.2 A Bank shall provide to a Customer who opens a cheque account, and to other Customers on request, general descriptive information on:

(i) the time generally taken for clearing a cheque and how a cheque may be specially cleared;
(ii) the effect of crossing a cheque, the meaning of "not negotiable" and "account payee only" and the significance of deleting "or bearer" when any of these expressions appear on a cheque;
(iii) how and when a cheque may be stopped;
(iv) how a cheque may be made out so as to reduce the risk of unauthorised alteration; and

(v) the dishonour of cheques, including post-dated and stale cheques.

PART B: PRINCIPLES OF CONDUCT

7.0 PRE-CONTRACTUAL CONDUCT

7.1 A Bank shall have readily available any Terms and Conditions of each Banking Service it currently offers to Customers or prospective Customers.

7.2 A Bank shall disclose the existence of any application fee or charge and whether the fee or charge is refundable if the application is rejected or not pursued.

7.3 Where a fee or charge is levied by a Bank for the provision of a bank cheque, a travellers cheque, an inter-bank transfer or the like service the Bank shall

disclose the fee or charge to a Customer upon request when the service is provided or at any other time.

8.0 OPENING OF ACCOUNTS

8.1 A Bank shall provide to a Customer or prospective Customer upon request general descriptive information (which may consist of or include material made available by a government) about the identification requirements of the *Financial Transaction Reports Act 1988 (Cth)* and the options available to the Customer or prospective Customer under tax file number legislation.

9.0 VARIATION TO TERMS AND CONDITIONS

9.1 When, in relation to a Banking Service, a Bank intends to introduce a fee or charge (other than a government charge referred to in section 9.2), or to vary the method by which interest is calculated or the frequency with which it is debited or credited, the Bank shall provide written notice of the change to each affected Customer at least 30 days before it takes effect.

9.2 A Bank shall notify affected Customers of the introduction or variation of a government charge payable directly or indirectly by its Customers by advertisement in the national media or local media or in writing to affected Customers, unless the introduction or variation is publicised by a government, government agency or representative body.

9.3 A Bank shall notify affected Customers of other variations to the Terms and Conditions (including a variation of Standard Fees and Charges or of an interest rate) in relation to a Banking Service by advertisement in the national media or local media or in writing to affected Customers, no later than the day on which the variation takes effect.

9.4 Unless otherwise agreed, a Bank may give any written notice to a Customer at his or her mailing address that was last recorded with the Bank. A Bank may require a Customer to notify the Bank promptly of a change to his or her name or address.

9.5 If a Bank considers there are sufficient changes to warrant doing so, the Bank will make available a consolidation of the Terms and Conditions applying to a Banking Service.

10.0 ACCOUNT COMBINATION

10.1 A Bank shall inform a Customer promptly after exercising the Bank's right to combine Accounts affecting the Customer.

10.2 In exercising a right to combine Accounts, a Bank shall comply with any applicable requirements of the Code of Operation for Social Security Direct Credit Payments.

11.0 FOREIGN EXCHANGE SERVICES

11.1 In providing a foreign exchange service, other than by credit or debit card or travellers cheque, a Bank shall provide to a Customer:

(i) details of the exchange rate and commission charges that will apply or, if these are not known at the time, details of the basis on which the transaction will be completed; and

(ii) an indication of when money sent overseas on the Customer's instructions would normally arrive at the overseas destination.

11.2 Prior to granting a foreign currency loan in Australia, a Bank shall provide to the Customer a general warning in writing of the risks arising from exchange rate movements and shall inform the Customer of the availability of mechanisms, if they exist, for limiting such risks.

12.0 PRIVACY AND CONFIDENTIALITY

12.1 A Bank acknowledges that, in addition to a Bank's duties under legislation, it has a general duty of confidentiality towards a Customer except in the following circumstances:
(i) where disclosure is compelled by law;
(ii) where there is a duty to the public to disclose;
(iii) where the interests of the Bank require disclosure; or
(iv) where disclosure is made with the express or implied consent of the Customer.

12.2 Subject to section 12.1, a Bank may not, without the consent of the Customer, disclose information concerning the Customer to another person but the Bank may disclose -
(a) to a Related Entity, information necessary to enable an assessment to be made of the total liabilities (present and prospective) of the Customer to the Bank and the Related Entity, and
(b) to a Related Entity of the Bank which provides financial services which are related or ancillary to those provided by the Bank, information concerning the Customer unless the Customer instructs the Bank not to do so. A Bank shall advise those who become Customers after it adopts the Code that they have the right to give this instruction by the means referred to in section 6.1(ii).

12.3 A Bank shall not collect information relating to Customers by unlawful means.

12.4 A Bank shall on request provide a Customer with information about that Customer which is readily accessible to the Bank and which may lawfully be provided. The information required to be provided is limited to the Bank's record of the Customer's address, occupation, marital status, age, sex, Accounts with the Bank and balances and statements relating to those Accounts (in this section 12 called "Customer information").

12.5 A Bank need not comply with a request under section 12.4 unless the Customer has, as clearly as possible, identified the Customer information requested and its likely location (if known to the Customer).

12.6 A Bank may recover its reasonable costs of supplying Customer information to a Customer.

12.7 A Customer of a Bank may request the correction of Customer information about the Customer held by the Bank.

12.8 A request for access to Customer information, or a request for the correction of Customer information, shall be dealt with in a reasonable time.

12.9 A Bank may not collect, use or disseminate information about a Customer's:
(i) political, social or religious beliefs or affiliations;
(ii) race, ethnic origins or national origins; or
(iii) sexual preferences or practices;
except that it may collect or use such information in accordance with this Code for a proper commercial purpose.

12.10 A Bank shall take reasonable steps to protect personal information held by it relating to a Customer against loss and against access, use, modification or disclosure that is unauthorised. A Bank shall require all staff with access to personal information concerning Customers to maintain confidentiality concerning that information.

12.11 In relation to a "banker's opinion" a Bank shall comply with any applicable requirements of any Credit Reporting Code of Conduct issued by the Privacy Commissioner under section 18A(1) of the *Privacy Act 1988 (Cth)*.

12.12 In this section 12 "Customer" includes an individual who would have been a Customer if this Code had applied at the time that individual acquired a financial service.

13.0 PAYMENT INSTRUMENTS

13.1 A Bank may inform a Customer of the advisability of safeguarding payment instruments such as credit and debit cards, cheques and pass books.

13.2 A Bank may require a Customer to notify the Bank as soon as possible of the loss, theft or misuse of his or her payment instruments.

13.3 A Bank shall inform a Customer of:

(i) the consequences arising from a failure by the Customer to comply with any requirement referred to in section 13.2 that is imposed on the Customer by the Bank; and

(ii) the means by which the Customer can notify the loss, theft or misuse of his or her payment instruments.

14.0 STATEMENTS OF ACCOUNT

14.1 At least every six months, a Bank shall provide a Customer with a record of all transactions relating to a deposit account of the Customer since the previous statement unless:

(i) a passbook is provided or it is agreed that other documentation will be the record of transactions on the deposit account;

(ii) there has been no transaction effected by the Customer on the deposit account during the past six months; or

(iii) the deposit account can be accessed by the combined use of a PIN and an EFT card (in which case the requirements of the Electronic Funds Transfer Code of Conduct apply).

15.0 PROVISION OF CREDIT

15.1 In considering whether to provide a Banking Service involving the provision of credit to a Customer, a Bank shall take into account the range of factors it considers are relevant to the Customer and the Banking Service to establish whether, in the Bank's view, the Customer has or may have in the future the capacity to repay. These factors may include:

(i) the Customer's income and expenditure;

(ii) the purpose of the Banking Service;

(iii) credit scoring (being a scoring method used by Banks to assess whether a credit applicant is an acceptable risk); and

(iv) the Customer's assets and liabilities.

16.0 JOINT ACCOUNTS AND SUBSIDIARY CARDS

16.1 A Bank shall provide to Customers opening a joint Account general descriptive information on:

(i) how funds may be withdrawn from the joint Account having regard to the instructions given by the Customers;

(ii) the manner in which such instructions can be varied; and

(iii) the nature of liability for indebtedness on joint account.

16.2 When accepting a Customer's instructions to issue a subsidiary credit or debit card, a Bank shall:

(i) provide general descriptive information to the primary cardholder on his or her liability for debts incurred by the subsidiary card holder by use of the card; and

(ii) inform the primary card holder of the means by which a subsidiary card may be cancelled or stopped and the fact that this may not be effective until the subsidiary card is surrendered.

17.0 GUARANTEES

17.1 This section shall apply to each guarantee and each indemnity (whether or not contained in a security) (called "guarantee" in this section 17) obtained from a third party who is an individual (called "the guarantor" in this section 17) for the purpose of securing any financial accommodation or facility provided by a Bank to any person (called "the borrower" in this section 17) other than -

(i) a public corporation or any of its Related Entities;

(ii) a corporation of which the guarantor is a director, secretary or member or any of its Related Entities;

(iii) a trustee of a trust (including a discretionary trust) of which the guarantor or a corporation or a Related Entity that is referred to in paragraph (ii) is a beneficiary or one of a class of beneficiaries under the trust; and

(iv) a partner, co-owner, agent, consultant or associate of any of the guarantor, a corporation or Related Entity referred to in paragraph (ii) or a trustee referred to in paragraph (iii);

at the time the guarantee is obtained. The term "public corporation" has the meaning set out in section 9 of the Corporations Law.

17.2 A Bank may only accept a guarantee if the amount of the guarantor's liability is limited to, or is in respect of, a specific amount plus other liabilities (such as interest and recovery costs) that are described in the guarantee.

17.3 Before accepting a guarantee a Bank shall inform a prospective guarantor that the documents specified in section 17.4(ii) and 17.6 will be provided to the prospective guarantor if the borrower consents. If the borrower does not consent, the Bank shall so inform the prospective guarantor and shall not accept the guarantee without the agreement of the prospective guarantor to proceed with the guarantee in the absence of such consent.

17.4 A Bank shall provide to a prospective guarantor -

(i) a written warning about the possibility of the prospective guarantor becoming liable instead of, or as well as, the borrower; and

(ii) subject to obtaining the consent of the affected borrower, a copy or summary of the contract evidencing the obligations to be guaranteed.

17.5 A Bank shall recommend that a prospective guarantor obtain independent legal advice.

17.6 Subject to obtaining the consent of the affected borrower, a Bank shall send to a guarantor:

(i) a copy of any formal demand that is sent to the borrower; and

(ii) on request by the guarantor, a copy of the latest relevant statements of account provided to the borrower, if any.

17.7 A guarantor may at any time extinguish the guarantor's liability to a Bank under a guarantee by paying to the Bank the then outstanding liability of the borrower to the Bank (including any future or contingent liability) or any

lesser amount to which the liability of the guarantor is limited by the terms of the guarantee or by making other arrangements satisfactory to the Bank for the release of the guarantee.

18.0 ADVERTISING

18.1 A Bank shall ensure that its advertising and promotional literature drawing attention to a Banking Service is not deceptive or misleading.

18.2 In any advertising in the print-media and any promotional literature that draws attention to a Banking Service and includes a reference to an interest rate, the Bank shall also indicate whether other fees and charges will apply and that full details of the relevant Terms and Conditions are available on application.

19.0 CLOSURE OF ACCOUNTS

19.1 Subject to the terms and conditions of any relevant financial service, a Bank:

(i) will upon request by the Customer close an Account of the Customer that is in credit;

(ii) may close an Account of the Customer that is in credit by giving the Customer notice that is reasonable in all the relevant circumstances and repaying the Customer the amount of the credit balance; and

(iii) may charge the Customer an amount that is a reasonable estimate by the Bank of the costs of closure.

PART C: RESOLUTION OF DISPUTES

20.0 DISPUTE RESOLUTION

20.1 A Bank shall have an internal process for handling a dispute between the Bank and a Customer and this process will be readily accessible by Customers without charge upon them by the Bank. A dispute arises where a Bank's response to a complaint by a Customer about a Banking Service provided to that Customer is not accepted by that Customer.

20.2 A Bank shall have available in branches general descriptive information on:

(i) the procedures for handling such a dispute;

(ii) the time within which the dispute will normally be dealt with by the Bank; and

(iii) the fact that the dispute will be dealt with by an officer of the Bank with appropriate powers to resolve the dispute.

20.3 Where a request for resolution of the dispute is made in writing or the Customer requests a response from the Bank in writing, the Bank shall promptly inform the Customer in writing of the outcome and, if the dispute is not resolved in a manner acceptable to the Customer, of:

(i) the reasons for the outcome; and

(ii) further action the Customer can take, such as the process for resolution of disputes referred to in section 20.4.

20.4 A Bank shall have available for its Customers free of charge an external and impartial process (not being an arbitration), having jurisdiction similar to that which applies to the existing Australian Banking Industry Ombudsman Scheme, for resolution of a dispute that comes within that jurisdiction and is not resolved in a manner acceptable to the Customer by the internal process referred to in section 20.1.

20.5 The external and impartial process shall apply the law and this Code and also may take into account what is fair to both Customer and the Bank.

Appendix H: Product Information

Please note that the following text is taken from vendor material, and the ABA makes no warranties as to the veracity of claims relating to performance and functionality. The order of listings does not indicate a preference or priority.

Hunter (Experian)

Hunter is a system that identifies potential fraudulent applications and highlights the highest risk applicants for the financial services and insurance industry. It can be used for any type of financial or insurance product including requests for mortgage finance, current accounts, card accounts, personal loans, insurance policy applications and claims, and instant credit applications.
http://www.experian.com.au/solutions/hunter1.pdf

Fraud-Check, Including Veri-Check (Baycorp)

FraudScore references the applicant's details against the FraudCheck database. A VeriCheck is performed concurrently verifying the applicant's name, address, phone number and drivers licence number against the Electoral Roll, Telephone Listings and the bureau file.
http://www.baycorp.com.au/

Fraudlink On-Us (Carreker)

Carreker's FraudLink On-Us™ is a comprehensive check fraud detection system that identifies counterfeit and forged checks with unmatched precision. Installed at more than 100 financial institutions worldwide, FraudLink On-Us has been proven to identify up to 80 percent of fraudulent on-us items, allowing most banks to realize a return on their investment within six months.
http://www.carreker.com/main/solutions/fraud_sol/fraudlink/on-us.html

Falcon Fraud Manager (Fair, Isaac)

Falcon Fraud Manager is a leading global payment card fraud detection system, monitoring more than 400 million payment card accounts worldwide. Current customers include more than 60% of the world's leading payment card issuers. Falcon Fraud Manager uses our proven neural network models and other predictive technologies to uncover payment card fraud in real time.

http://www.fairisaac.com/page.cfm/section=sub_cat/id=552/id3=552/id1=63/id2=202/layout=layout1.cfm?CFID=1023709&CFTOKEN=45081927

Falcon Fraud Manager for Merchants (Fair Isaac)

The system allows the setting of threshold levels to accept, reject or seek additional information on an order and automatically execute the appropriate action. To enhance the Falcon Fraud Manager score, fraud managers can easily create and deploy fraud management policies with the Policy Management Subsystem. And with the Order Management Workstation, customer service representatives can focus their attention where human intervention is most appropriate, enabling the company to save valid orders identified as high risk, increase sales and improve customer satisfaction.
http://www.fairisaac.com/page.cfm/section=sub_cat/id=552/id3=552/id1=63/id2=202/layout=layout1.cfm

CardAlert (Fair, Isaac)

CardAlert® Fraud Manager For ATM Deposits

For either the EFT network provider or card issuer, CardAlert Fraud Manager for ATM Deposits monitors high-risk deposits and withdrawals for signs of fraud on a daily basis. Upon detecting a problem, CardAlert Fraud Manager immediately reports the information to the organization. The institution can then take timely action to prevent fraudulent withdrawals or reverse them soon after they occur and prior to posting, thereby avoiding possible long-term, sustained losses from ATM deposit fraud.

http://www.fairisaac.com/page.cfm/section=sub_cat/id=529/id3=529/id1=63/id2=202/layout=layout1.cfm?CFID=1023709&CFTOKEN=45081927

Alert Systems (CO-OP Network)

The function of the CO-OP Network Alert System is to protect institutions from major ATM/debit card fraud. The system involves a three-tier process:

- Card Alert reduces and prevents losses from counterfeit ATM/debit card schemes
- Deposit Alert identifies potentially fraudulent ATM deposit activity
- Cardholder Usage Monitor Report provides a highly customized profile of each credit union's EFT activity

By working in tandem, the three systems control both institution and cardholder losses.
http://www.co-opnetwork.org/public//Media/med_product_overview.cfm

Verified by Visa

Verified by Visa is a secure and easy to use service that gives extra protection when shopping online, by means of a personal password.
http://www.visa.com.au/verified/index.shtml

SecureCode (Mastercard)

MasterCard® SecureCode™ provides an additional layer of security for online purchases by helping to prevent unauthorized individuals from using a MasterCard card to buy online.
http://www.mastercard.com/au/cardholderservices/securecode/

Hotscan (Logica CMG)

Hotscan, Logica's automated transaction scanning software, satisfies the OFAC regulations as well as each firms defined risk control procedures by providing a comprehensive, fully featured compliance system, running in real time.
Because it can accept traffic from multiple hosts and can be scaled to accommodate increased traffic flows, one Hotscan application can provide a central real-time transaction filtering process. In addition, the Hotscan Customer Account Scanning System (CASS) allows the Institution to scan new and existing accounts against currants watch lists in a batch mode.
http://www.logica.com/pdf/launderingWP.pdf