NSW GOVERNMENT | Justice

Background paper: plastic card fraud

May 2011

Table of contents

1. Introduction

Plastic payment cards provide a convenient and generally secure medium with which people conduct a wide variety of transactions. Their convenience, in conjunction with mass advertising, has seen a steady growth in both the volume and value of plastic card transactions over the past decade. However, with new commercial opportunities comes new crime opportunities, and there appears to be a continual struggle between the financial industry, law enforcement and the offenders as technological advancements in security in the plastic card industry, are met with more innovative and adaptive advances to plastic card crime.

Previously Australia was thought to be 'lucky' due to its geographical distance from other countries that experienced higher fraud incidents. However, international travel and the advancement in technology have meant that Australia has become a prime target for fraud offenders, as evidenced by the rise in plastic card fraud.

The financial industry and law enforcement is currently invested in strategies to reduce card fraud and identify and prosecute offenders. However, these strategies need to be continually evaluated for their effectiveness in the current situation and there may be an opportunity to build on them. Fraud trends in Australia tend to mirror those overseas. Therefore, prevention strategies should consist of lessons learnt from other countries, and include a clear investment in a long-term fraud prevention strategy that seeks the cooperation between the public and private industry.

2. Plastic card transactions

Plastic cards such as ATM cards, debit and credit cards are by far the most common non-cash payment method used by Australian consumers today. These cards are used for in-store purchases (where the store has an EFTPOS[1] terminal), to withdraw cash from an automatic teller machine (ATM), or in the case of debit and credit cards, to make purchases over the phone or Internet.[2]

In the context of plastic card transactions, Australia has three main payment systems:

- ATM card – a card that allows the consumer to make purchases from a savings or transaction account using their own funds. An ATM card requires a personal identification number (PIN) when making purchases or withdrawing funds.
- Debit card – a card that allows a consumer to make purchases from a savings or transaction account both in Australia and overseas. A debit card requires the consumer to enter a PIN, provide a signature or quote the card details.
- Credit card – a card that allows the consumer to establish a line of credit with the card issuer for purchases both in Australia and overseas. Similar to a debit card, these cards require the consumer to enter a PIN, provide a signature or quote the card details. There are also credit charge cards such as American Express and Diners Club.

[1] Electronic Funds Transfer at Point of Sale.
[2] APCA Annual Review 2010.

In recent years, Australia has seen advancements in technology in the banking industry that allow for faster, more convenient and more secure payment systems, such as the Europay, MasterCard and Visa (EMV) computer chip identification system. This system in particular comes in two distinct types *contact*, which require physical contact with the reader; and, *contactless*, which uses radio frequency (RF) technology.[3]

- Contact computer chip identification commonly refers to Chip and PIN technology. In 2009, companies such as Visa and Mastercard commenced rolling out in Australia credit and debit cards (scheme cards) that feature an embedded microchip. The chip and pin technology allows the card to be inserted into the ATM in lieu of swiping the magnetic stripe, and payment is completed upon entering the PIN.
- Contactless payment refers to recent initiatives such as Visa Paywave and Mastercard Paypass. Scheme cards, key fobs and mobile phone devices embedded with the technology are held over a card reader within close range, to make a purchase of up to $100 without the need to provide a signature or enter a PIN.

Newer payment systems such as chip and pin have assisted in improving customer efficiency and reducing some types of card fraud such as skimming (discussed in Section 3), however, it is important to also consider what further opportunities are created by the technology for fraud offenders, who are constantly seeking better ways to exploit weaknesses in the system. For example, whereas previously financial institutions were more likely to be targeted given they held large amounts of cash, criminals may now be more likely to focus their attention on the individuals carrying these cards and other devices, as another avenue to obtaining card details, effectively shifting the risk from the bank to the consumer.

A further example is the uptake of contactless payment using mobile phones. Also referred to as 'mobile wallets' and 'e-purse systems' this payment system may also provide opportunities for fraud (discussed in Section 4).

The emerging technology in payment systems highlights the need for key stakeholders to invest locally in a long-term fraud prevention strategy. Furthermore, existing fraud prevention measures should be continuously evaluated to ensure their relevance to the current climate and to close any gaps that can provide criminal opportunity.

3. Use of plastic cards in Australia

The growth in plastic card transactions has steadily increased over the past decade. From the period 2000 to 2010, the number of monthly ATM withdrawals rose from 41.5 million to 68.4 million with the value of these transactions in 2010 estimated to be $12 billion dollars.

However, the biggest increases were in EFTPOS and credit card transactions. Over the past decade, the number of EFTPOS transactions per month more than tripled by the year 2010, with an average increase of 25 per cent per year (Table 1). Also, as shown in Table 2, the number of credit card transactions has more than doubled with the value of these transactions estimated to be at $19.6 billion per month in 2010.

[3] Hutchings, A. (2010). *Review of Computer Chip Identification Systems*, ARC Centre of Excellence in Policing and Security, Briefing Paper Sept 2010, Issue 1.

Table 1 Card transactions (monthly)

	ATM withdrawals transactions per month	EFTPOS transactions per month	Credit cards transactions per month
2010	68.4 million	183.8 million	131.0 million
2009	70.8 million	165.0 million	118.8 million
2008	72.9 million	144.6 million	119.0 million
2007	72.0 million	121.9 million	118.3 million
2006	68.3 million	108.5 million	115.7 million
2005	64.3 million	98.1 million	102.9 million
2004	61.6 million	87.4 million	93.6 million
2003	59.8 million	81.0 million	85.5 million
2002	57.3 million	75.6 million	83.7 million
2001	45.3 million	53.2 million	67.8 million
2000	41.5 million	48.5 million	61.9 million

Table 2 Card transactions – value (monthly)

	ATM withdrawals value of transactions – dollars per month	EFTPOS value of transactions – dollars per month	Credit cards value of transactions – dollars per month
2010	12.0 billion	12.0 billion	19.6 billion
2009	12.4 billion	11.3 billion	17.8 billion
2008	12.5 billion	9.8 billion	18.3 billion
2007	12.2 billion	8.2 billion	17.4 billion
2006	11.5 billion	7.4 billion	16.5 billion
2005	10.6 billion	6.6 billion	14.2 billion
2004	10.2 billon	5.8 billion	12.8 billion
2003	10.0 billion	5.4 billion	11.4 billion
2002	9.8 billion	4.9 billion	10.9 billion
2001	8.0 billion	3.2 billion	8.0 billion
2000	6.9 billion	2.9 billion	7.0 billion

Source: APCA.

The information in the tables highlight the strong growth in both the volume of card usage and the values of card transactions. As we continue to move towards a cashless society it is important to examine the use of non-cash payments systems such as plastic cards with a view to understanding it in the context of fraud. The following section provides an overview of plastic card fraud in Australia with an emphasis on the two most prevalent types of fraud; card-not-present and counterfeit fraud.

4. Plastic card fraud

What is plastic card fraud?

Plastic card fraud is defined as using plastic payment cards, such as ATM, debit, credit or store cards to take money without permission or prior knowledge from a bank, building society or credit card account (or to charge money to credit/debit cards).[4]

In the context of the above definition, plastic card fraud commonly occurs through the illicit acquisition and/or use of card information and the personal identification number (PIN).

Prevalence

Data on the prevalence and nature of plastic card fraud in Australia is not readily available and understandably so. Plastic card fraud data is likely to contain sensitive information that can be misused by offenders, who may learn new techniques to exploit the system, or create unnecessary public fear and deter legitimate activity.

Financial institutions do not generally report the annual number of incidents of bank transaction card fraud or the total amount of money defrauded. The financial institutions have passed this responsibility by collectively setting up an organisation called the Australian Payments Clearing Association (APCA) that is owned by member financial institutions. To its credit, APCA reports national credit card fraud, debit card fraud and cheque fraud figures, providing aggregate data for each year.

At present, data obtained by APCA is likely to be the best estimate of the prevalence of plastic card fraud in Australia. Currently APCA represents the four big banks in Australia, including the Australia and New Zealand Banking Group Limited (ANZ), Commonwealth Bank, National Australia Bank Limited and Westpac Banking Corporation.[5] Research bodies such as the Australian Institute of Criminology when reporting on prevalence use figures from APCA.[6]

APCA categorises plastic card fraud into six types. These include, lost/stolen card, card never received, fraudulent application, counterfeit/skimming, card not present (CNP) and other (where the fraud cannot be categorised under any of the other fraud categories).

The graph below provides a summary of the type of plastic card fraud reported by APCA in 2009. Card not present where the account information is used without the physical card being involved or the authority of the cardholder, accounted for just over 50 per cent of all reported fraud. Counterfeit/skimming incidents were the second largest category accounting for 32 per cent of all fraud.

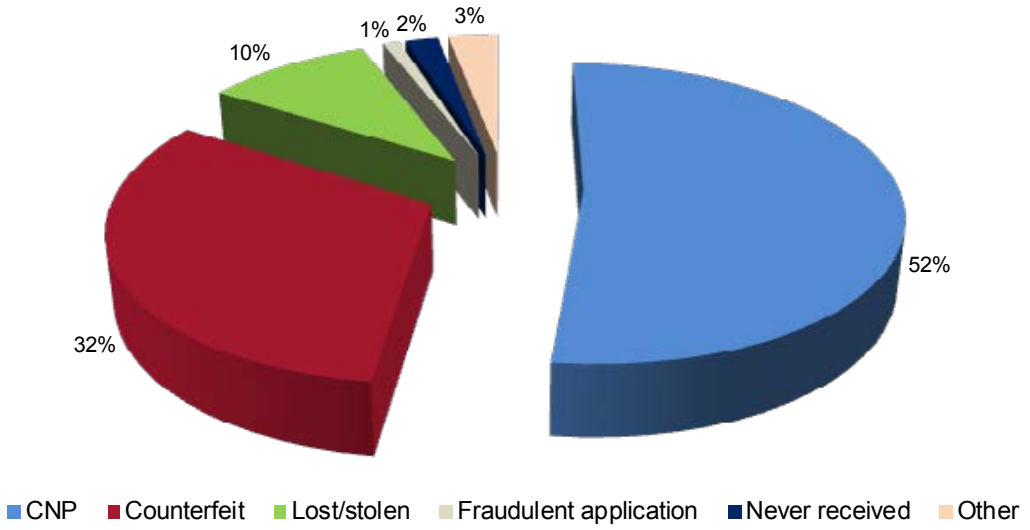
---

[4] Moon, D., Flatley, J., Hoare, J., Green, B. & Murphy, R. (2010). *Acquisitive crime and plastic card fraud: Findings from the 2008/09 British Crime Survey*, Home Office Statistical Bulletin.

[5] List of all the major Australian financial organizations that are members of APCA can be found at http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/MemberList_OwnerMembers

[6] Smith, R. (2010) *Risks and responses to fraud in Australia*, Australian Institute of Criminology. http://www.aic.gov.au/about_aic/research_programs/staff/~/media/conferences/other/smith_russell/2010-11-risks.pdf

Figure 1 Australian Plastic Card Fraud Type 2009



Source: AIC

Card not present fraud

Card not present (CNP) most commonly involves the theft of genuine card details that are then used to make purchases over the Internet, by phone or mail order. The genuine cardholder may not be aware of this fraud until they check their statement.[7] This category also includes fraud where a card should normally be present (e.g. in a retail transaction) but a merchant has chosen to accept the transaction based on a card number only and it turns out to be a fraudulent transaction.[8] Methods used to obtain card details typically include data hacking or through unsolicited emails or telephone calls.

As shown in Table 3, APCA reported an increase in card-not-present fraudulent transactions between 2007 and 2010. Between 2009 and 2010, APCA estimated that over $100 million had been defrauded through card-not-present transactions perpetrated in Australia and overseas on Australian-issued cards. Also noteworthy is that the number of fraudulent transactions has increased by almost 100 per cent from 2007/2008 to 2009/2010 and that the majority of fraud is occurring overseas on Australian-issued cards.

Table 3 Card not present fraudulent transactions perpetrated in Australia or overseas on Australian-issued cards

Category	2007–2008		2008–2009		2009–2010	
	No	A$	No	A$	No	A$
In Australia	80,643	26,732,131	97,813	29,487,263	145,045	36,764,843
Overseas	175,548	46,027,508	235,841	52,867,452	362,146	65,818,873
Total	**256,191**	**$72,759,639**	**333,654**	**$82,354,715**	**507,191**	**$102,583,716**

Source: APCA

[7] Financial Fraud Action UK, 2010, *Fraud The Facts 2010, The Definitive Overview of Payment Industry Fraud and Measures to Prevent It*, Financial Fraud Action Group UK.
[8] APCA, 2010, *Payment Fraud Statistics Methodology Paper*, APCA.

Counterfeit/skimming

Counterfeit card fraud is the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and changes to the details on the face of the card with intent to defraud. Most of this fraud involves a technique called skimming.

Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value – CVV) from a valid card. Information may then be encoded on a counterfeit or stolen card and used fraudulently.[9]

According to APCA, almost $35 million was skimmed from Australian-issued credit, debit and charge cards both in Australia and overseas in the financial year from 1 July 2009 to 30 June 2010. This is a reduction from the previous financial year where an estimated $45 million was skimmed between July 2008 to June 2009. The reduction is thought to be due to financial institutions responding to a series of skimming attacks on ATMs and EFTPOS terminals during 2009, as well as the progressive rollout of chip technology, which has seen a reduction in skimming fraud on Australian-issued credit cards.[10]

Table 4 Counterfeit/skimming transactions perpetrated in Australia or overseas on Australian-issued cards

Category	2007–2008		2008–2009		2009–2010	
	No	A$	No	A$	No	A$
In Australia	32,572	18,786,287	33,305	19,602,649	25,052	12,179,609
Overseas	35,921	24,183,691	39,385	25,652,738	51,506	22,285,235
Total	68,493	42,969,977	72,690	45,255,387	76,558	34,464,844

Source: APCA

Prevalence in New South Wales

In April 2010, the Crime Prevention Division (CPD) of the Department of Attorney General and Justice (DAGJ) commissioned a victimisation survey to identify the extent of card fraud in NSW in the last two years. The survey collected data from a representative sample of 2000 people, thus the results could be generalised to the entire NSW population.

The survey collected data on four types of card fraud; robbery at an ATM, card skimming, card-not-present fraud and theft of a card. Overall 9.2 per cent (n = 182) of the sample reported having been a victim of one or more of the offences in the past two years. The most common offences reported were card-not-present fraud followed by card skimming. This data is consistent with APCA's fraud data regarding the most prevalent types of fraud in Australia as mentioned above.

Noteworthy in relation to card skimming was that more residents reported being a victim in the past two years than in the years prior, suggesting that this crime may be increasing. Furthermore, 25 per cent of respondents who had their card skimmed, reported it as having occurred at an EFTPOS device. This data contributes to the body of research that EFTPOS skimming is an emerging problem.

[9] APCA, 2010, Payment Fraud Statistics Methodology Paper, APCA.
[10] APCA Annual Review 2010.

While there were few significant differences between gender, those aged 25-54 were significantly more likely than younger or older respondents to have experienced one or more of the offences. Few respondents reported the offence to Police.

Information sharing

At present, there appears to be some sharing of information between financial institutions and law enforcement (more than 657,000 cases of card fraud were reported in Australia in 2009).[11] However, the situation is complicated as in the event of a fraud, customers are encouraged to report the matter to their bank, reducing the possibility that the matter would be reported to Police.

APCA advises their fraud data is representative of the entire market. However, membership is voluntary, therefore it is not known whether all financial institutions are members of APCA, and further how the non-member financial institutions (if any) report on the problem of fraud.

To understand the full extent of the problem, their needs to be a clear investment in an information sharing and reporting service between key stakeholders as seen in countries such as the UK. Such a system would provide the banking industry, law enforcement and other key stakeholders with cases and trends of card fraud to assist in coordinating resources as part of a long-term fraud prevention strategy. The Commonwealth Attorney General's Department is currently leading the development of such a system.

Furthermore, an information-sharing system would also keep consumers, as potential victims, aware of recent issues in payment fraud and the available prevention measures. A survey of 2,000 residents in NSW conducted on behalf of CPD, found that while two in three respondents were aware that many cards now have a computer chip, only 20 per cent were aware that the chips are designed to improve card security. This highlights the need for more education regarding the option for consumers to upgrade their card to chip, and commence using a PIN in lieu of a signature.

5. How plastic card fraud is committed

The emerging technology in payment card systems means offenders are constantly seeking innovative ways to commit card fraud. Typically card and PIN details are obtained either through cyber crime, ATM machines and more recently, EFTPOS terminals and mobile phone devices. Below is a list of some of the techniques employed by card fraud offenders.

Cyber crime

In 2009, Internet fraud accounted for 58 per cent of card-not-present losses in the UK, up from 55 per cent in 2008.[12] The data for Australia is not readily available, however, card usage over the Internet has also increased rapidly in Australia and therefore we can expect the results to be the same as in the UK. The two main methods for obtaining card details by cyber criminals are malware (malicious software) attacks and phishing.

---

[11] Australian Crime Commission (2011) *Organised Crime in Australia*, Australian Crime Commission.

[12] Financial Fraud Action group UK, 2010, *Fraud the Facts 2010, The Definitive Overview of Payment industry Fraud and Measures to Prevent it*, Financial Fraud Action Group UK.

- Malware (including keyloggers and spyware) has consistently been ranked as one of the key cyber threats to the financial industry.[13] Spyware is installed on a victims computer and with the use of a keylogger allows a criminal to not only spy on what websites are visited, but also record what keys are pressed such as online banking passwords. This data is then sent back through the Internet to the criminal. Spyware and keyloggers are most commonly installed by sending a link to the victim's computer in the form of a spam email. Spyware can also be installed when a victim visits a website or downloads music.[14] In response to this, a number of organisations such as Symantec conduct publicity campaigns to sell Internet security that reduces the likelihood of a computer being infected.
- Phishing refers to online scams that frequently use unsolicited messages purporting to originate from legitimate organisations, particularly financial services. Victims are deceived into disclosing their financial and/or personal identity information to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information).[15] Statistics from the Anti-Phishing Working Group (APWG) (2009), Symantec (2010) and Microsoft (2010, 2009) indicated that the financial industry was the most targeted industry sector of phishing attacks in the 2009 calendar year.

The NSW Registry of Births, Deaths and Marriages of DAGJ launched an identity fraud campaign in 2010 to address the problem of phishing in relation to identity theft. The campaign aims to educate the public on keeping personal documents secure and to also be vigilant of email phishing, a common method used to capture information.

In addition, the Australian Federal Police (AFP) Joint Banking and Financial Sector Investigation team investigates cyber crime. The team was formed in 2004 and consists of bank staff seconded to the AFP to assist police investigations. The team is supported by the Australian Bankers Association, an organisation funded by member financial institutions that aims to ensure the banking industry views are put forward when Government determines policy or legislation.

Overall, the increasing transfer of everyday activities to the Internet such as banking and shopping has created further opportunities to commit fraud.[16] In addition, the influx of social networking sites such as Facebook and Twitter provide cyber criminals with access to a wealth of personal information. Results from the Consumer Fraud in Australasian survey undertaken by the Australian Institute of Criminology in 2008 and 2009 found that email was still the primary medium through which people receive scam invitations. The survey also found that there was a significant relationship between the ages of the victim and whether they were scammed, and further that raising awareness of scam types could be an effective way to reduce victimisation. Consideration should therefore be given to developing further consumer awareness campaigns that are targeted towards at-risk groups.

---

[13] Choo, K. (2011), *Cyber threat landscape faced by financial and insurance industry*, Trends and Issues Paper No 408, Australian Institute of Criminology, Canberra.

[14] Scamwatch Australia http://www.scamwatch.gov.au/content/index.phtml/itemId/694322

[15] Choo, K. (2011), *Cyber threat landscape faced by financial and insurance industry*, Trends and Issues Paper No 408, Australian Institute of Criminology, Canberra.

[16] Budd, C. & Anderson, J. (2011). Consumer Fraud in Australasia: Results of the Consumer Fraud Taskforce online Australia surveys 2008 and 2009, Australian Institute of Criminology, Technical and Background Paper 43.

Mobile phone devices

The increase in ownership of smart phones, coupled with the introduction of mobile banking applications and the use of mobile phone devices for contactless payments, has meant that more consumers are able to conduct financial transactions (including making payments) using their phone. The disadvantage, however, is that it provides another avenue for cyber criminals to obtain consumer's bank details.

In April this year, Symantec released the findings of its Internet Security Threat report, which found "attackers are exhibiting a notable shift in focus towards mobile devices",[17] and further cyber criminals are likely to develop even more threats targeting smart phones in the future. In the last year, Symantec released a product, Norton M*obile Security*, which provides consumers with anti-malware functionality for mobile phones as well as providing the ability to remotely lock or wipe a device in the case of theft or loss.

Therefore, as mobile phone handsets become more sophisticated, the issue of theft will become more important as handsets contain more and more sensitive information. In the UK, in response to Government and law enforcement concerns around a possible crime spike from the introduction of contactless payments on mobile phones, the UK Cards Association and mobile phone industry have together developed a preliminary list of best practice guidelines for their respective industries. Given card fraud trends here tend to mirror international markets, it would seem that Australia is in a prime position to also develop industry guidelines in preparation for contactless payment using mobile phones.

Automatic teller machines

Some of the common ways ATMs are targeted include:

- Lebanese loop is where a device is inserted into an ATM's card slot, which retains the card inside the cash machine. The victim is then tricked into re-entering their PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.
- Skimming consists of two components. The first part is the skimmer itself, a card reader placed over the ATM's real card slot. When consumers pass their card through the counterfeit reader, it scans and stores all of the information on the magnetic strip. Secondly, cameras – hidden or near the ATMs are positioned to get a clear view of the keypad and record all of the ATM's PIN action. Or another method used to capture PIN numbers is the use of a fake keypad in lieu of a camera where skimming keypads are designed to mimic the keypad's design. Upon gaining these details, 'skimmers' will either use the detail to make a counterfeit card which can then be used either in Australia or overseas, make withdrawals from the bank account at other locations or use the details to make purchases in retail outlets or over the internet.
- Cash Trapping is similar to the Lebanese Loop, however, instead of capturing a card, a device is slipped into the cash dispenser, which prevents cash from being withdrawn. After the cardholder leaves, the thief removes the device and steals the cash.

[17] Symantec Internet Security Threat Report, Volume 16.

- Shoulder surfing refers to when criminals watch the cardholder entering the PIN, then steal the card using distraction techniques or pick pocketing, before using the stolencard and genuine PIN.

Anecdotal information from the NSW Fraud Squad suggests that in relation to ATMs, machine focused fraud such as skimming is the most common method for criminals to illegally obtain card details in Australia. It would be valuable to find out whether other forms of fraud such as cash trapping which have been prevalent in England, Scotland and Ireland are also expected to occur in Australia, lending further support for a fraud information-sharing and reporting service. Further information regarding the security of ATMs is discussed in Section 5.

EFTPOS crime

EFTPOS devices

For EFTPOS skimming to occur, criminal's capture an individual's card details and PIN by either stealing a terminal, making changes to it and putting it back or replacing a genuine EFTPOS device with a tampered device which looks and works like a normal EFTPOS device.

In response to a series of skimming attacks on EFTPOS devices in Australia in 2009, APCA designed and developed an education campaign for merchants with the support of the Australian Crime Commission and Australian Federal Police. The initiative, Safeguard Against Skimming consisted of a training video and brochure and advised merchants on how skimming occurs and how they can detect and prevent EFTPOS fraud on their premises.[18] It would be valuable to find out whether the campaign has been effective in contributing to the reduction in the value of skimming transactions in the last financial year, as previously shown in Table 4.

EFTPOS security

EFTPOS Payments Australia Limited (EPAL) maintains the standards for EFTPOS devices in Australia. The standards provide a set of rules for the technical, operational and security requirements of EFTPOS devices. Currently all EFTPOS devices are approved by APCA, however, it is not known whether or how the standards are enforced. Further, these standards do not relate to the physical security (i.e. environmental considerations) of the device.

As mentioned previously, a retail focused education initiative to reduce EFTPOS fraud was rolled out in 2010 as a joint initiative between the banking industry and Police. It would appear that a coordinated approach between the banking industry, law enforcement and merchants is a significant step in the right direction to addressing what is considered to be a growing problem. Further, it would appear that identifying which retailers, when and how they are targeted would be essential when developing crime prevention strategies.

[18] A copy of the brochure can be found here http://www.apca.com.au/merchanteducation2011//PublicME_SkimmingBrochure.pdf

6. Automatic teller machine security

Frauds attacks on ATMs are a worldwide problem. ATM fraud is growing because it produces cash and is considered to be fairly low risk relative to other crimes.[19] The necessary equipment for criminal activity is inexpensive, readily available and expendable. ATM fraud also lends itself to organised crime. The fraud is repeatable, profitable and does not appear likely to end. The example below presented by Diebold, one of the main manufactures of ATMs in Australia, highlights the increasing global nature of ATM fraud.

> In 2006, Russian police arrested a group of criminals accused of stealing at least $500,000 from US bank accounts in a cross border ATM scam. The gang obtained stolen account information and PINs from organised crime groups in the US, Canada, and France to make fraudulent cash withdrawals at ATMs in Moscow. The funds were stolen from the accounts of US citizens who had never been to Russia.[20]

According to APCA, the number of ATMs in Australia is at an all-time high, with 28,764 recorded in June 2010. It is understood that there are approximately seven manufactures that supply ATMs to Australia. The requirements for ATM machines supplied in Australia are discussed in detail in the following section.

Minimum standards for ATMs

The minimum requirements for ATMs in Australia are set locally by APCA and globally according to the Payment Card Industry (PCI) standards. These standards relate mostly to the hardware and software of the ATM machines, as opposed to physical ATM security.

APCA standards

In the year 2000, the Australian Payments Clearing Association established the Consumer Electronic Clearing System (CECS), which primarily involves setting minimum standards in relation to the physical and logical (software) security of ATM terminals and EFTPOS devices.[21] APCA provides a list of approved devices, however, note that due to continual review, devices on the list may not longer be compliant or may not be compliant in the future.

APCA advised anecdotally that while they recommend the same security on all ATM terminals and EFTPOS devices, the actual implementation of security by manufactures is generally different. Information obtained anecdotally from a consultant in payment security confirmed this and suggested that while ATMs and EFTPOS manufactures are in theory required to comply with APCA's standards, there is no actual enforcement of these requirements. Noteworthy is that membership to APCA is voluntary, and therefore it is not known whether all of the manufactures of terminals are members of APCA, and further whether they are aware of the standards and subsequently compliant.

---

[19] Diebold. (n.d) *White Paper: ATM Fraud and Security*. Retrieved 5 April 2011, from http://www.diebold.com/atmsecurity/files/DBD_ATMFraud_WP.pdf

[20] ibid.

[21] The CECE manual which outlines the standards can be found at http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/CECS_Manual.pdf/$File/CECS_Manual.pdf

PCI standards

The PCI Security Standards are technical and operational requirements set by the Payment Cards Industry Security Standards Council to protect credit card data. Broadly PCI standards globally govern all merchants and organisations that store, process or transmit credit card data. There are also specific requirements for software developers and manufactures of devices used in the transaction process. In the context of ATM terminals and EFTPOS devices, PCI standards currently relate only to the software and the keyboard of the machine, with no considerations for the design or physical security such as environmental aspects, lighting, etc.

Compliance with the PCI security standards is enforced by the major payment brands who established the Council; American Express, Discover Financial Services, JCB International, Mastercard Worldwide and Visa Inc. Therefore while the PCI Security Standards Council sets the standards for PCI security, each payment card brand has its own program for compliance. For example, Visa advises that if a member does not comply with the security standards or fails to rectify a security issue, they may receive a fine.

ATM physical security

There are several types of ATM security ranging from digital and physical security to maintaining the integrity of a transaction, how the device operates and finally customer identity and safety. Global organisations such as the ATM Industry Association and the UK ATM Security Working Group have developed best practice guidelines that discuss the mitigation of skimming and other crimes, and also consider environmental factors such as risk assessments, site selection, lighting, etc, however, similar to standards relating to the software and hardware of machines, they are not enforceable.

Globally ATM manufactures have implemented a range of technologies to deter criminals. These include, closed circuit television video (CCTV) surveillance, remote monitoring, PIN pad shields to obscure data entry, encrypted PIN pads, changes to the ergonomic design of the ATM to prevent shoulder-surfing, consumer awareness mirrors, consumer education and a variety of methods to prevent card skimming as listed below:

- jittering – a process that controls and varies the speed of movement of a card as it is swiped through the card reader, making it difficult to read the card data
- alert systems – systems that monitor routine patterns of withdrawal and notify operators or financial institutions in the event of suspicious activity
- chip-based cards – these cards house data on microchips instead of magnetic stripes, making data more difficult to steal and cards more difficult to reproduce
- foreign object detection – this type of technology can alert owners, operators, or law enforcement in the event that a skimming device is added on the fascia of an ATM.[22]

Information obtained from Diebold, one of the main suppliers of ATMs in Australia, indicates that the market for the manufacture and supply of ATM terminals is categorised as either high-end or low-end. High-end machines are considered to have a higher investment in security and are generally used by the banks and areas with high traffic such as shopping

[22] Diebold. (n.d) *White Paper: ATM Fraud and Security*. Retrieved 5 April 2011, from http://www.diebold.com/atmsecurity/files/DBD_ATMFraud_WP.pdf

centres, whereas the low-end machines can be seen in convenience stores and petrol stations. Currently, we are not aware of any data that identifies which of these terminals are targeted more frequently and how often security for terminals is upgraded.

The minimum standards for the manufacture and supply of ATMs in Australia are complex. While there are standards in place for the logical and physical security of ATMs they do not appear to be consistently enforced. Given the wide variety of ATMs, the unique characteristics of each installation and the crime considerations at each location, it is difficult to standardise effective prevention strategies. However, minimising losses, mitigating risks and maintaining consumer confidence in the ATM channel are logical priorities for financial institutions and others who deploy ATMs. Therefore, enforceable standards that regulate the manufacture and supply of ATMs should be considered as part of a multi-layered approach in card fraud prevention.

7. Offenders

Information regarding who commits card fraud is scant. This is likely to be due to the low level of detection and prosecution of offenders. Unlike 'traditional' crimes, where offenders and victims need to be at the same place and the same time, card fraud offenders can attack their victims on other continents and further they do not need to physically steal cards.

In the following discussion, card fraud offenders are separated into two categories; low-skilled and high-skilled offenders (i.e. those individuals involved in organised crime).

Low-skilled offenders

The ease with which software used in skimming can be generated makes card fraud a lucrative business for opportunistic low skilled criminals. Offenders need only to download credit card generating software and obtain a device for skimming over the Internet. Further to this, criminals without strong technological skills can obtain ready-made malicious software packages online that will enable them to commit a range of offences. Research has found, however, that the skill 'entry' requirements are rising as more sophisticated technology is introduced by the financial sector.

High-skilled offenders

According to the Australian Crime Commission, Australian and transnational organised crime groups are involved in card fraud. The groups may be involved in either skimming card data in Australia and withdrawing cash overseas, or skimming data overseas and withdrawing cash in Australia. Organised crime groups also recruit financially vulnerable individuals to participate in shopping holidays to Australia, using fraudulent or stolen credit cards. In addition, card fraud offenders have their own supply and demand in the underground economy for stolen credit card information.[23] For example, Symantec estimates that credit card data can be bought for as little as $0.07 to as much as $100 per piece on the underground black market.

[23] Wilson, S. (2008), Cardless Criminals: Card-Not-Present Fraud is Spiraling Out of Control, with Very Few Options for Stopping It, Online Banking Review, April/May, p 5.

Overall, card fraud appears to consist of a number of related activities with different modus operandi, knowledge and skill requirements. In relation to who commits card fraud, many studies on card fraud rely on the victim side for data information as part of the self-reporting mechanisms. Data in relation to fraudulent transactions on Australian-issued cards (as discussed previously in Section 3) indicates that the majority of card fraud occurs overseas, lending further support to the evidence that this crime is most likely committed by organised groups. Therefore perhaps another avenue is to interview the actual offenders who are committing these crimes to provide a better insight into this type of fraud.

8. International card fraud prevention

United Kingdom (UK)

The UK Cards Association, the leading trade association for the cards industry in the UK reported total fraud losses on UK cards fell by 28 per cent between 2008 and 2009 and continued to fall in 2010. This is the first time that card fraud has decreased since 2006. The downward trend is thought to be due to ongoing initiatives by the banking industry such as better awareness by retailers about how to protect their chip and PIN equipment from criminal attacks,[24] greater sign-up to online fraud prevention initiatives such as MasterCard Secure Code and Verified by Visa by cardholders and retailers, improved industry sharing of fraud data and intelligence, increasing use of fraud detection tools by banks and retailers as well as the increasing roll-out of Chip and PIN abroad and on UK cards.

At an industry level, a number of units have been established in the UK to tackle plastic card fraud. The Financial Fraud Action Group UK is the name under which the financial services industry co-ordinates its activities on fraud prevention. It represents a united front against financial fraud and works in partnership with the UK Cards Association and other key stakeholders on industry initiatives to prevent fraud.

In 2002, the Dedicated Cheque and Plastic Crime Unit (DCPCU) was established as a special unit to tackle the organised gangs responsible for the majority of the UK's cheque and card fraud. The unit is sponsored by the banking industry.

Furthermore in 2008, a Fraud Intelligence Sharing System (FISS) was established to enable the banking industry to share information on all confirmed, attempted and suspected fraud in the UK. The system provides the banking industry with a secure and robust reporting mechanism, as part of their long-term fraud prevention strategy.

Canada

According to the Royal Canadian Mounted Police, in 2008 counterfeit credit card use represented the largest category of credit card fraud with an estimated loss of approximately $196 million. Studies suggest that as Europe commenced implementing chip and pin technology, criminals migrated to Canada to commit card fraud. As a result, card issuers have commenced rolling out chip and pin technology in Canada to reduce the opportunity for fraud. Card issuers such as Visa and MasterCard have set deadlines for the implementation of chip and pin and announced that following the deadlines, the liability for fraudulent transactions will shift to merchants that have not implemented the technology.

[24] Information for retailers can be found at http://www.financialfraudaction.org.uk/Retail-Introduction.asp

With regards to prevention, the banking industry's crime investigation and prevention activities are coordinated through the Canadian Bankers Association's Bank Crime Prevention and Investigation Office (BCPIO). Canada also runs a month long education campaign each year in March to improve consumers' awareness and understanding of the dangers of fraud. The campaign has been adopted around the world, including Australia. Every March the Australasian Consumer Fraud Taskforce coordinates an information campaign for consumers, including National Consumer Fraud Week.

United States of America

The United States does not have a system to collect and report aggregate fraud loss information. Available sources on payment fraud either only target specific groups and are therefore narrowly focused or for some reason are incomplete. Furthermore, the financial industry is yet to adopt chip and pin technology, most likely due to the estimated cost when compared with their current level of fraud.

However, while countries like the UK are focused on updating their chip and pin technology, the United States appears to be more compliant to PCI standards to ensure all companies that process, store or transmit credit card information maintain a secure environment. In June 2009, Nevada, US, became the first state to mandate compliance to PCI standards making it a legal requirement. Furthermore, there appears to be more investment in addressing identity fraud with the establishment of the President's Identity Theft Taskforce and the Federal Trade Commission which focus on three key areas; law enforcement, education and Government regulations.

Analysis

Thus, international fraud prevention measures appear to vary based on the level and type of fraud in each country. The implementation of Chip and PIN technology in many countries, for example, has caused geographical displacement (e.g. from one country to another) and tactical displacement (e.g. from skimming/counterfeit card fraud to online card fraud) of credit card fraud.

Countries such as the United Kingdom and United States have improved their fraud prevention strategies by enhancing their coordination between the public and private industry. The establishment of the President's Identity Theft Taskforce in the United States and the Fraud Intelligence Sharing System in the United Kingdom are evidence of the banking industry, law enforcement and Government working together in addressing fraud problems.

Australia has to date invested in a range of strategies to reduce card fraud. However, coordination among key stakeholders is integral to any fraud prevention strategy to ensure resources are used effectively and efficiently.