Trends in Smartcard fraud[•]

Susan Burns, George R. S. Weir

Department of Computer and Information Sciences, University of Strathclyde,
Glasgow G1 1XH, UK
{susan.burns, george.weir}@cis.strath.ac.uk

Abstract. The introduction of smartcard technologies has reduced the incidence of card fraud in the UK, but there are still significant losses from fraudulent card use. In this paper we detail the context of smartcard introduction and describe the types of fraud that remain a threat to cardholders and other stakeholders in the card system. We conclude with a risk analysis from the cardholder's perspective and recommend greater cardholder awareness of such risks.

Key words. Smartcards, fraud, consumer security, risk assessment.

1. Introduction

A recent report from the European Security Transport Association (ESTA) found that nearly 20% of the adult population in Great Britain has been targeted as part of a credit or debit card scam. As a result, the UK has been termed the 'Card Fraud Capital of Europe' [1], with UK citizens twice as likely to become victims of card fraud as other Europeans. Plastic card fraud is a lucrative exploit for criminals and the proceeds may be used to fund organised crime. Smart payment cards (Chip and PIN cards) were introduced in the UK to replace magnetic stripe cards and support PIN verification of card transactions. By the end of 2005, more than 107 million of the 141.6 million cards in the UK had been upgraded to smart cards [2]. Levels of plastic card fraud fell by 13% to £439.4 million in 2005 [3] and again to £428 million in 2006 (Figure 1). The reduction has been widely attributed to the rollout of smart cards with Chip and PIN authentication.

If the media is to be believed, the UK introduction of Chip and PIN authentication for credit and debit card transactions is flawed and has failed to reduce levels of card fraud across the board. Specific cases highlighting the security implications of smart card based technology have been widely reported, including exploits at Shell petrol stations [4] and Tesco self-service tills [5].

As cards are a widely accepted international form of payment, fraud can happen virtually anywhere in the world or on the Internet. Cards can be compromised in the

[•] Presented at the 4th International Conference on Global E-Security, University of East London, June 2008.

UK and then used overseas. Cardwatch research shows that most of the fraud committed abroad on UK cards affects cards that have been compromised in the UK [3].

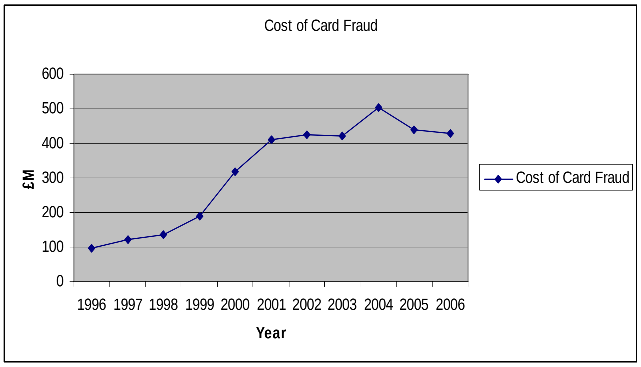

Figure 1 - Trends in Plastic Card Fraud Levels [6]

Although the financial cost of card fraud is largely borne by the banking industry, the cardholder experiences loss of time in taking steps to resolve matters, as well as inconvenience, worry and frustration while a fraudulent incident is investigated. The cardholder's credit rating can be affected and the whole affair can be a distressing experience. Figure 2 shows that levels of international fraud have risen for UK issued cards, while they have fallen for UK transactions.

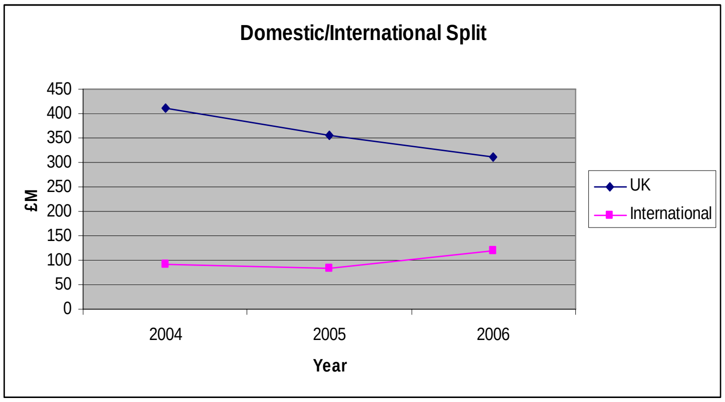

Figure 2 - Domestic and International Split of Fraud on UK Issued Debit and Credit Cards [6]

2. Types of Card Fraud

The UK Payments Association (APACS) has identified five categories of card fraud:

- Counterfeit Card Fraud,
- Skimming,
- Mail Non Receipt,
- Lost and Stolen Fraud,
- Card not Present.

Levels of these frauds on UK issued cards are shown in Figure 3.

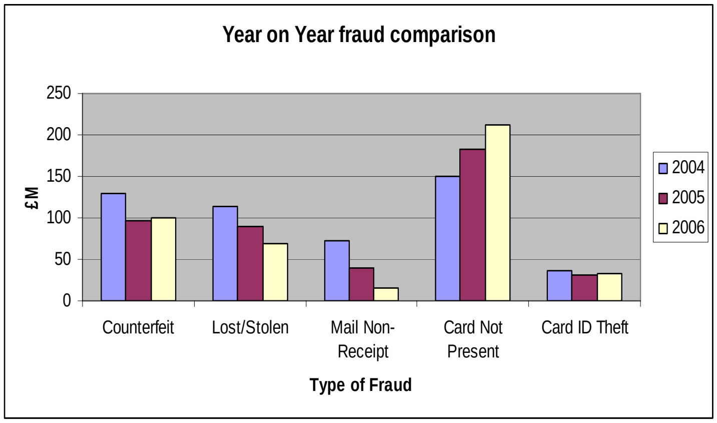

Figure 3 - Levels of Plastic Card Fraud on UK Issued Cards 2004-2006 [6]

2.1 Counterfeit Card Fraud

Counterfeit cards are also referred to as cloned cards. Counterfeit cards are made by altering and re-coding validly issued cards or by printing and encoding cards without permission from the card issuing company. Most cases of counterfeit fraud involve skimming of valid card details, a process whereby the genuine card details from the magnetic stripe are electronically copied onto another card, without the legitimate cardholder’s knowledge. In most cases, the cardholder will be unaware that their card details have been skimmed until card statements reveal that illicit transactions have been made on their account.

2.2 Skimming

Skimming of card details can happen at retail outlets where a corrupt employee can put a card through a skimming device which will copy data from the card’s magnetic stripe so it can be used to encode a counterfeit card. Skimming can also occur at cash machines where a skimming device has been fitted. A skimming device is attached to the card entry slot where it records the electronic details from the magnetic stripe on the back of the inserted card. A separate pin-hole camera is hidden to overlook the PIN entry pad to record the PIN number. Fraudsters can then produce a counterfeit card for use with the captured PIN to withdraw cash at a cash machine.

Criminals can also shoulder surf, whereby they watch the user entering a PIN and then steal the card for their own use. Another type of device can be inserted into a cash machine where it will trap the inserted card. A fraudster can then suggest retrying the PIN. Once the genuine cardholder gives up and leaves to contact the card issuer or cash machine operator, the criminal can then remove device, retrieve the card and then use it with the PIN details they have observed.

2.3 Lost and Stolen Fraud

This type of fraud occurs when a card is lost by the cardholder or is stolen from them. Fraudsters can then use the card to obtain goods and services. Once the cardholder notices their card is gone, they will contact the card issuer but as it can take time to realise the card has gone, most fraud of this type takes place before the card has been reported as lost or stolen.

Levels of this type of fraud have remained static for the past five years but the introduction of Chip and PIN is expected to reduce this by making it more difficult for fraudsters to use a lost or stolen card in person at a retail outlet. Prior to Chip and PIN, the retailer would verify that the signature on the sales voucher matched that written on the back of the card. The signature strip was signed by the cardholder in ink and was subject to wear and tear over the lifetime of the card.

2.4 Mail Non-Receipt

This occurs where a card is stolen when it is in transit from the issuing bank or building society to the cardholder. This is similar to lost and stolen fraud since it takes time for the cardholder to realise that a card has not arrived. This delay is often compounded by the fact that cards are often sent out automatically by the issuers rather than at request of the cardholder, e.g. when a card is nearing its expiry date. Card issuers have endeavoured to reduce levels of this type of fraud by using secure mail services and/or requiring the cardholder to phone and activate the card before it can be used. However, fraudsters could still intercept cards in transit and skim the details before re-mailing them to the cardholder. Once the cardholder activates the card, the fraudster can also use the counterfeit card produced using the skimmed details.

Credit card cheques, often sent to cardholders on an unsolicited basis by the card issuing company, also offer criminals an additional means of obtaining unauthorised spending against a card account.

2.5 Card Not Present

This type of fraud covers any card transactions where the cardholder is not physically present, i.e. those conducted over the internet, telephone, fax and mail order, and is now the largest type of card fraud in the UK [6]. Fraudsters obtain details of a card, i.e. cardholder name, card number and the 3 digit security number from the back of the card, and can use these to pay for goods or services over the internet, phone, fax or mail order. Companies reliant on Card Not Present (CNP) transactions are unable to check the physical security features of the card to determine if it is genuine and cannot rely on signature or PIN authentication. Equally, there is no check that the information is being provided by the genuine cardholder.

2.6 Card ID Theft

Identity theft occurs when a criminal obtains an individual's personal information and uses this to open or access card accounts in that individual's name. A criminal may use stolen documents such as utility bills and bank statements, or false documents, to give the necessary documentation to open up a card account. Alternatively, they can use key bits of personal information to take control of an account, perhaps arranging for payments to be taken from the card account or by changing account address details and requesting issue of cheques or a new card.

2.7 Likely Trends

Wilhelm [7] considered the future of credit and debit card fraud due to the introduction of smart cards and predicted a hybrid period of approximately ten to fifteen years during which magnetic stripe and smart card technology would co-exist. In this period, fraudsters will get creative and exploit technology and social conditioning to devise attacks on chip technology.

One of the highlighted concerns is allowing the use of the magnetic stripe as a fallback where a chip fails to function. This permits fraudsters to circumvent a number of the safeguards provided by smart card technology. This will prevent Chip and PIN from fully addressing counterfeit card fraud made possible through the theft of card details in transit or from lost/stolen scenarios. While the report predicts that a significant reduction in card counterfeiting is likely to occur, it acknowledges that while magnetic stripes are available, counterfeiting remains a viable option for fraudsters. The report also highlights that fraudsters will focus their efforts on CNP fraud and target merchants as a vulnerable link in the process.

3. Stakeholders

Although cardholders are usually the focus of concern in matters of card fraud, there are other stakeholders in the establishment, use and maintenance of smartcards. These stakeholders are (1) cardholders; (2) merchants; (3) Acquirers; and each of these has roles, responsibilities and risks in operation of the card system.

Research indicates that we can all do more to defeat criminals, particularly where basic security measures are involved. Statistics, such as the following [8], are particularly alarming and highlight the need for cardholders to be aware of the risk and impact if they fail to protect their PIN number and card details:

- 25% of all UK residents have disclosed their PIN to someone else, exposing them to heightened risk of fraud and potentially making them liable for any card fraud losses they may suffer;
- 27% of Britons use the same PIN for all their cards and the average adult has four cards each;
- 44% of people still allow their cards out of their sight (in restaurants and bars for example) when settling a bill;
- 51% of online shoppers do not fully appreciate that the start of a website address changes from ‘http’ to ‘https’ when they enter a website made secure for purchasing.

The key recommendation for cardholders is that they should be security conscious and take all practical precautions when undertaking a card payment. Cardholder complacency is still a large factor in card fraud levels. While card issuers are unlikely to acknowledge vulnerabilities, in order to avoid adverse reputational impacts, increased cardholder awareness of the risks and impacts associated with known vulnerabilities in the Chip and PIN system, will ensure that they become less complacent.

The large variety of card terminals makes it difficult for a cardholder to identify one that has been tampered with, but there are other ways they can notice fraudulent actions, for example by being familiar with merchant best practices. This would allow them to raise alarms with other staff members if suspicious behaviour is observed, e.g., swiping a card prior to inserting it into a card terminal or watching a PIN being entered. Cardholders should also check their credit card and current account statements to identify any illicit transactions. One measure to limit exposure for a debit card linked to a current account is to establish a second account containing a smaller balance for use in card transactions

The agreements which merchants have with their acquirers spell out the terms under which they can accept card payments. The terminals supplied by the acquirers determine floor limits and undertake the Chip and PIN authorisation process. Vulnerabilities exist when fraudsters have access to terminals and so merchants should seek to address and improve staff awareness of process vulnerabilities that could lead to card fraud through training. Staff should be trained in card transaction processes and be empowered to request additional authorisation via a Code 10 call where they deem necessary and know how to do this without putting themselves at risk.

Merchants must also be alert to the fact that they are a prime target for fraudsters. They have a responsibility to be vigilant and monitor transactions and any suspicious staff activities. References should be checked when hiring new staff. Systems holding customer and transaction data must be adequately protected. Any concerns raised by customers about staff undertaking card transactions should be investigated. Card present merchants have various ways of reading and processing card details e.g. staff inserts card, cardholder inserts card or card is swiped and this can make it difficult for cardholders to know what would constitute a suspicious action by a member of staff.

Acquirer guidelines should be followed to minimise the risk of chargeback for both card present and CNP transactions. The planned rollout of ‘contactless’ cards in the UK towards the end of 2007 may introduce further concerns for merchants as only one in three low value transactions would be flagged for verification by PIN. For a CNP merchant there are specific challenges as Chip and PIN is not currently an option for this type of transaction and it is an area where card fraud has risen significantly.

The Address Verification System (AVS) allows retailers to verify the billing address supplied with that associated with the cardholder and Card Security Code (CSC) allows retailers to cross check a special security code held on the back of the card. Card schemes are also introducing positive identification measures such as Verified by Visa and MasterCard Secure Code to help merchants. Merchants should protect themselves against chargeback's by introducing these measures for on-line transactions. By 30th June 2007, all CNP merchants must have introduced this measure or at least have a plan in place to do so. Chargeback of disputed transactions is likely for any non-compliant merchants.

The acquirer or merchant acquirer is the bank retained by the retailer to process payment card transactions on their behalf. Acquirers are responsible for paying the merchant for the transactions they process. They do this on receipt of card transaction details from retailers by passing them to the card issuer for authorisation and processing. Acquirers are also responsible for obtaining transaction authorisation prior to the delivery of goods and/or services.

The responsibility for maintenance and upgrades to card terminals also lies with acquirers who risk who must provide clear instructions and guidelines to merchants in order to minimise instances of card fraud and chargeback. Acquirers are increasingly using fraud detection software to detect patterns that could be due to fraudulent activity. This can be helpful in identifying and investigating unusual patterns of transactions.

4. Risk Assessment

Security is a balance between confidentiality, authentication and integrity versus convenience, cost and reliability. Figure 4 illustrates the balance that must be struck by stakeholders when implementing technical solutions to counter security vulnerabilities, essentially this boils down to cost versus benefits.

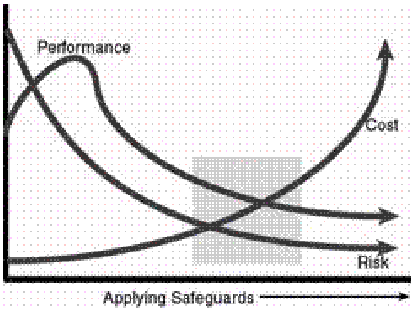

Figure 4 - Risk Management Payoffs [9]

This generic approach can be applied to security measures for smart card payments, whereby:

- Cost is the amount it costs the card issuer and card scheme to support the plastic card payments, including the cost of implementing changes to the system e.g. longer keys or moving to online authentication to validate all card transactions;
- Performance considers convenience and reliability e.g. avoiding reputational damage or inconvenience for customers or retailers;
- Risk is remaining level of risk which the security measures have not fully mitigated. This could be financial loss, additional costs, loss of market share, reputational damage, corporate embarrassment, legal or regulatory investigation or risk to personal safety.

The potential loss or exposure from a given risk can be reduced through assessing and management of the risk (Figure 5). Effective risk reduction methods may leave an element of residual risk, but will bring benefits, although these may not always be financial, e.g., they could be reputational benefits.

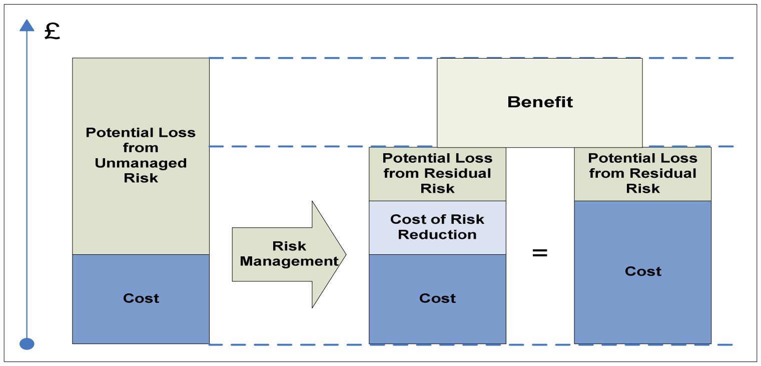
£
Potential Loss from Unmanaged Risk
Cost
Risk Management
Benefit
Potential Loss from Residual Risk
Cost of Risk Reduction
Cost
=
Potential Loss from Residual Risk
Cost

Figure 5 - Risk Management

A risk map is a technique to analyse and illustrate risks, likely causal events and potential impacts [10]. The links shown are not always exhaustive but demonstrate the potentially wide ranging impacts of each risk and support analysis of outcomes and mitigation actions. As a tool, they also allow flexibility to consider how the impact of one risk, e.g., card stolen, can be compounded by the occurrence of other risks, such as the PIN having been obtained.

Figure 6 illustrates a risk map analysis for the cardholder, based upon four primary risk conditions, card obtained by fraudsters, card details obtained by fraudsters, PIN obtained by fraudsters, and PIN forgotten by cardholder. The associated cardholder events represent the contexts in which the risks are created, and the impact arising from these circumstances is also indicated.

For the cardholder, the key risks centre on the components for which the cardholder is responsible, namely the smartcard, the PIN and documents such as statements and receipts that contain card details. The events include some that are within the cardholder's control, e.g., keeping a note of the PIN number, but others such as a compromised terminal are beyond cardholder control.

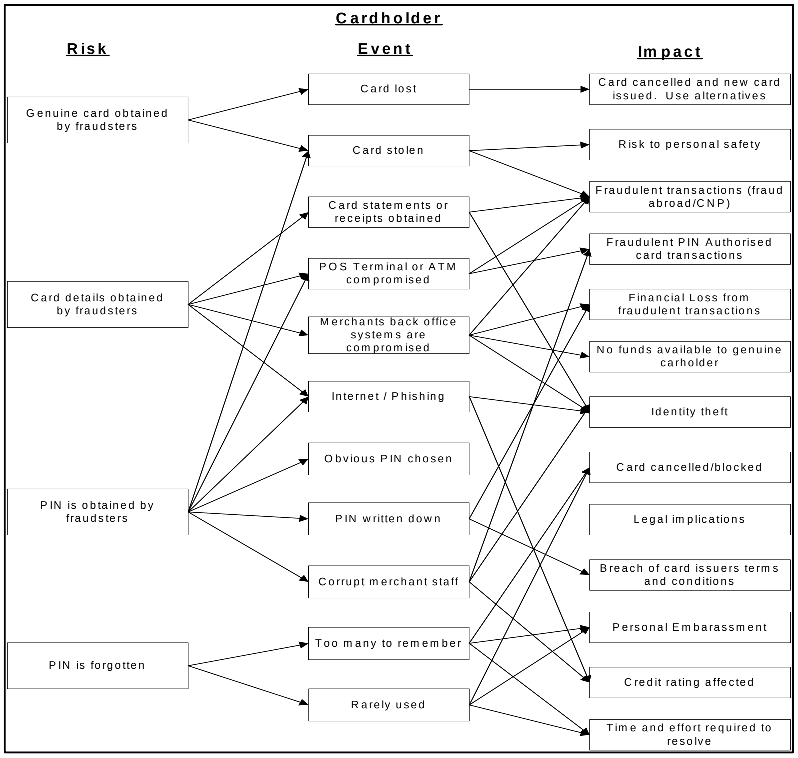
Cardholder
Risk
Event
Impact
Genuine card obtained by fraudsters
Card details obtained by fraudsters
PIN is obtained by fraudsters
PIN is forgotten
Card lost
Card stolen
Card statements or receipts obtained
POS Terminal or ATM compromised
Merchants back office systems are compromised
Internet / Phishing
Obvious PIN chosen
PIN written down
Corrupt merchant staff
Too many to remember
Rarely used
Card cancelled and new card issued. Use alternatives
Risk to personal safety
Fraudulent transactions (fraud abroad/CNP)
Fraudulent PIN Authorised card transactions
Financial Loss from fraudulent transactions
No funds available to genuine carholder
Identity theft
Card cancelled/blocked
Legal implications
Breach of card issuers terms and conditions
Personal Embarassment
Credit rating affected
Time and effort required to resolve

Figure 6 - Risk Map for Cardholder

5. Summary and Conclusions

The introduction of smartcards to the UK marketplace has had a significant effect in reducing the incidence of card fraud, but further steps are required to prevent continued instances of fraud. A key step in this direction is to clarify the roles, responsibilities and risks faced by the different stakeholders in the card process. Furthermore, 'awareness raising' in which cardholders become more conscious of their risks and responsibilities may afford the best defence against consumer fraud. Our analysis of the card process, stakeholders and cardholder risks may contribute to this awareness.

References

1. This Is Money. UK is ‘Card fraud capital’. 2006. Available from: http://www.thisismoney.co.uk/credit-and-loans/idfraud/article.html?in_article_id=414834&in_page_id=159. Last accessed 21/03/2008.
2. APACS. Plastic Cards, 2006. Available from: http://www.apacs.org.uk/payment_options/plastic_cards.html. Last accessed 21/03/2008.
3. Cardwatch. The cost of card fraud, 2006. Available from: http://www.cardwatch.org.uk/default.asp?sectionid=5&pageid=123. Last accessed 21/03/2008.
4. BBC. Petrol firm suspends chip-and-pin, 2006. Available from: http://news.bbc.co.uk/1/hi/england/4980190.stm. Last accessed 21/03/2008.
5. BBC. Thieves 'cash in at Tesco tills', 2006. Available from: http://news.bbc.co.uk/1/hi/business/5406742.stm. Last accessed 21/03/2008.
6. APACS. One year anniversary of Chip and PIN change over - UK leads the way in Chip and PIN rollout, 2007. Available from:. http://www.apacs.org.uk/media_centre/press/07_14_02.html?print=yes&print=yes. Last accessed 21/03/2008.
7. Wilhelm, W, K. Payment Card Fraud in a Chip Card World – examining potential changes in card fraud in the near future, FairIsaac, March 2003. Available from: http://www.fairisaac.com/NR/rdonlyres/7CE35A4B-96B0-43A0-9503-78BDAC483510/0/PaymentCardFraudWP.pdf. Last accessed 21/03/2008.
8. RBS. Fraudwatch Newsletter, No 23, Royal Bank of Scotland, Dec 2006.
9. McCumber. *Assessing and Managing Security Risk in IT Systems*. Auerback Publications, CRC Press Florida, USA, 2005.
10. Buchanan S. and Gibb, F. The information audit: methodology selection. *International Journal of Information Management*, 2008.