Legal and Regulatory Update

Chip and spin: Shifting burdens and new threats in retail card fraud

Shelagh Gaskill, Gavin McGinty and James Pratt

Received: 6 June 2005

Shelagh Gaskill
is a partner in the Outsourcing, Technology and Commercial group of Pinsent Masons, an international law firm. Shelagh specialises in information law relating to the commercial exploitation of data of all types, including their acquisition, sale and exchange. She also specialises in the legal aspects of the establishment and design of databases, worldwide and group company data flows and data protection and privacy laws in the UK, Europe and third world countries. She is one of the UK's leading data protection specialists.

Gavin McGinty
is a solicitor in the Outsourcing, Technology and Commercial group at Pinsent Masons. Gavin is a specialist in the regulatory issues relating to e-commerce and the internet, and the use of new media technology in the financial services industry.

James Pratt
is a trainee solicitor in the Outsourcing, Technology and Commercial group at Pinsent Masons. He advises clients on all aspects of information technology and e-commerce law, and has a particular interest in retail marketing.

Keywords: credit, card, fraud, retail, chip, PIN

Shelagh Gaskill
Pinsent Masons
30 Aylesbury Street
London EC1R 0ER, UK
Tel: +44 (0)20 7490 4000
Fax: +44 (0)20 7490 2545
E-mail: shelagh.gaskill@pinsentmasons.com

Abstract

The technical security of data transfer over the internet has improved dramatically in recent years. The result is that those most vulnerable from online fraud are not the individuals having their card details intercepted and used, but the merchants who are faced with fraudsters buying goods with stolen cards or using stolen identities. The recent introduction of chip and PIN will not reduce the overall level of card fraud, but it will shift its impact from traditional retail to online or mail order.

Introduction

The introduction of chip and PIN has been widely proclaimed by banks and the consumer credit industry as a panacea to credit and debit card fraud. But recent figures published by APACS[1] indicate that levels of card fraud are going up rather than down. On its own, the introduction of chip and PIN as a new secure method of payment will not succeed in eliminating card fraud. It will merely result in a shift in the levels of fraud from traditional retail to card-not-present (CNP) transactions. Tied to the introduction of chip and PIN, card issuers have shifted liability for fraud on to merchants who do not, or cannot, use the new system. This means that online and other merchants who rely on CNP transactions must employ additional security methods, as it is they who will bear the costs of card fraud.

Card fraud in the UK

UK credit card fraud cost industry £504m in 2004, according to APACS, the UK payments association. This was an overall increase of 20 per cent on fraud levels in 2003.[2] CNP fraud accounted for the single largest proportion of this figure, with losses up 24 per cent to £150.8m compared to £122.1m in 2003. CNP transactions are those carried out where the card is not physically present at the point of sale — ie where only the card number and expiry date are provided. CNP transactions are the most common method of card use for telephone, mail order and internet sales.

Counterfeit card fraud increased slightly, up 17 per cent to £129.7m in 2004 from £110.6m in 2003.[3] A counterfeit (or cloned) card is one that has been printed, embossed or encoded without permission from the issuer, or one that has been validly issued and then altered or recoded. Most cases of counterfeit fraud involve skimming, a process whereby the genuine data on a card's magnetic strip are electronically copied on to another without the cardholder's knowledge. The cloned card is then used in normal retail sales, although of course the same data could also be used for CNP sales. An alarming new threat is the use of cloned cards to withdraw money from ATMs, where the fraudster is also aware of the PIN for the card. Finding out a cardholder's PIN is made more likely with the advent of chip and PIN cards, where cardholders are asked to enter their PIN numbers in full view of others in a variety of public places like shops and restaurants. Cardholders are often unaware of counterfeit fraud until a statement arrives showing purchases or withdrawals they did not make.

Fraud on lost and stolen cards increased by a modest 2 per cent to £114.4m compared to £112.4m in 2003.[4] Most fraudulent activity of this type takes place before the cardholder has reported the loss or theft, and will increasingly rely on CNP transactions where the criminal is not aware of the PIN.

Spiralling card fraud rates

ATM fraud showed the most significant increase over the year, jumping 81 per cent to £74.6m, a rise from £41.1m in 2003.[5] Criminals commit fraud at cash machines in a number of ways. 'Shoulder surfing' is the term used to describe the activity where criminals look over a cardholder's shoulder to watch the PIN being entered, then steal the card and make fraudulent transactions on the account. Obviously with the advent of chip and PIN this same technique can now be used at places other than just ATMs. Fraudsters may also use skimming devices attached to the card entry slot and miniature cameras overlooking the PIN pad. These enable the criminal to produce counterfeit cards and withdraw money at cash machines using a legitimate PIN.

ID theft associated with cards has also grown over the past two years — up 22 per cent from £30.2m in 2003 to £36.9m in 2004.[6] ID theft on cards occurs when a criminal uses fraudulently obtained personal information to open or access card accounts in someone else's name. Types of ID fraud include 'application fraud', where the criminal uses stolen or false documents to open an account in someone else's name, and 'account take-over fraud', where the criminal gathers personal information about an account holder and then contacts the card issuer, masquerading as the genuine cardholder, reporting the card lost and requesting a replacement to be sent to a new address.

Another type of fraud which showed a marked increase on 2003 was so-called 'mail-non-receipt fraud'. This type of fraud occurs where cards are stolen in transit — after card issuers send them out and before the genuine cardholders receive them. APACS' figures show that losses from this type of fraud grew sharply from 2003 — up by 62 per cent to £72.9m.[7] This was probably a direct result of the rollout of the new chip and PIN programme, which put 3 million cards in the postal system in September 2004 alone.

There are two clear conclusions which can be drawn from these statistics. The first is that card fraud is continuing to rise. More importantly, however, the most significant rises are in areas where the introduction of chip and PIN is likely to have little or no effect. In particular, CNP fraud and ATM fraud are both growing faster than the underlying rate of growth in card fraud generally.

Chip and PIN

What is chip and PIN?

Chip and PIN was launched in the UK in October 2003 in an attempt to tackle the growing problem of credit and debit card fraud. The scheme was intended to become widely operational on 1 January 2005. The banking community hopes that by the end of 2005 most credit and debit card transactions where the customer is present during the transaction will involve authentication by chip and PIN.

Chip and PIN requires card users to authenticate their identity at the point of sale by keying in a four-digit PIN, instead of signing on paper. Newly issued credit and debit cards contain chips using encryption methods which check and authenticate the PIN number when transactions are processed. Since the launch of chip and PIN in October 2003 more than 94 million chip and PIN cards have been issued. More than three-quarters of all cardholders have at least one chip and PIN debit or credit card in their wallets. As a result, over 50 chip and PIN transactions are now taking place every second.[8]

Improving authentication and tackling counterfeit cards

The technology behind chip and PIN in the UK is the EMV card payments system. It has been designed by Europay, Mastercard and Visa. There are two facets to the chip and PIN system. The chip seeks to make it more difficult for criminals to produce counterfeit cards by ensuring that the card is genuine. The PIN seeks to ensure that the person presenting the card for payment in a particular transaction is the true owner.

The cardholder verification method (CVM) system determines how a cardholder proves ownership of his or her card when seeking to make a transaction. The chip card and the point-of-sale terminal both maintain a list of methods of identification that they find acceptable, PIN number now being the most common, followed by signature. On each transaction, the point-of-sale terminal will typically ask for a PIN entered by the customer to be verified by the card. The chip verifies the PIN that has been entered and the transaction can proceed. The argument runs that since a PIN cannot be forged in the same way as a signature this will cut the level of fraud where the customer and the card are present at the point of sale.

Chip and PIN is also intended to make it harder for criminals to produce counterfeit cards. The designers of the EMV technology have concentrated on making the new chip cards as difficult to counterfeit as possible. Once the card has verified the PIN, the terminal sends a summary of the transaction data and the card produces a ‘transaction certificate’ attesting to its authenticity — an electronic key to match the authorising key held by the issuing bank. Provided the point-of-sale terminal is connected to the issuing bank via a network, the bank can then read the transaction certificate and prove that the card is genuine.

Experience of chip and PIN in the UK

So much for the rhetoric. As a technical process how effective is chip and PIN at achieving what it is designed to do — reducing card fraud?

Underpinning the security of all card transactions is the principle of authentication. Authentication is the process by which an individual's entitlement to access a service is authorised by reference to one or more authenticating factors. Authenticating factors typically rely on something which the user knows (eg a PIN or a password), something which the user possesses (eg a smart card or other token) or something which the user is (eg a biometric identifier like a fingerprint). Establishing what level of authentication is appropriate should relate to the potential harm which could arise as a result of misuse. Therefore, the higher the risk of fraud to a card user or merchant, the greater the need for effective authentication of a card transaction.

Limitations of chip and PIN

While an improvement on signatures, chip and PIN does not provide a particularly high degree of authentication certainty. The chip is designed to demonstrate that the person is in possession of a valid card, and the PIN demonstrates that he knows the 'unique' number associated with the card. But the card and the PIN could easily fall into the hands of another individual, and there is nothing which physically links the card and the PIN to the individual presenting the card. In other words, in respect of the technology available, chip and PIN provides a low degree of certainty that the individual using the card is the person who is meant to be using it.

From a technological perspective, some critics argue that chip and PIN technology is not as secure as the banking industry would like to suggest.[9] They speculate that the CVM system by which the PIN operates may be susceptible to modification. In theory it is therefore possible for a fraudster to take a stolen chip card and reprogramme the chip so as to have the terminal believe that a signature is all that is required. They also suggest that particular anti-counterfeiting techniques used in the current chip and PIN technology can be overcome if point-of-sale terminals are offline. Because chip and PIN does not rely at all times on online authentication, many transactions will take place offline, with the retailer only going online when a card requires. In many cases, therefore, there will be no way of telling if the card is genuine on the spot.

Fraud displaced to CNP

Most significantly, current chip and PIN technology is only designed to tackle certain types of card fraud. Even if it is accepted that chip and PIN will succeed in reducing levels of counterfeit card fraud and fraud on lost and stolen cards, the figures show that even taken together these types of fraud constitute less than half (48 per cent) of all card fraud in the UK.[10] Chip cards do nothing to combat the most common type of card fraud, CNP fraud. Chip and PIN is not likely to reduce overall levels of card fraud, but merely displace card fraud from traditional retail environments into CNP transactions.

CNP fraud

CNP most commonly involves the theft of genuine card details, which are then used to make purchases through a remote channel such as by phone, fax, mail order or over the internet. As with counterfeit fraud, genuine cardholders will still have possession of their cards, so may not be aware of this fraud until they check their statements.

Currently when a CNP transaction is processed the merchant requests authorisation from the card issuer. This authorisation simply confirms that the card has not been reported lost or stolen and that there are sufficient funds in the account. It does not confirm that it was the genuine cardholder who supplied the details. The merchant accepting CNP transactions is responsible for ensuring the transaction is not fraudulent. If it is fraudulent, the full amount may be charged back to the merchant.

Authentication problems in the CNP environment

The incidence of this type of fraud has grown in recent years alongside an increase in online transactions. According to figures published in November 2004 from both the Office for National Statistics and Visa,[11] UK online sales figures doubled between 2003 and 2004. But the increase in CNP fraud is not solely attributable to the internet — and indeed most CNP fraud occurs through transactions made over the phone or by mail order.[12]

The problem in countering CNP fraud is that neither the card nor the cardholder is present at the point of sale. This means that:

- CNP merchants such as mail order or online retailers cannot check the physical security features of a card to determine whether it is genuine
- without a signature or a PIN it is difficult to confirm whether or not the customer is the legitimate cardholder
- card issuers cannot guarantee that the information provided in a CNP transaction relates to the genuine cardholder.

Fraud on lost and stolen cards and mail-non-receipt cards will often also lead to CNP fraud. Unless the criminal has been able to obtain the PIN (eg by shoulder surfing the cardholder at a shop before stealing the card), it is not as easy as wandering down to the nearest bank with a lost or stolen card and withdrawing money. It used to be the case that the criminal could practise the signature on the back of the card and then make as many purchases as possible in shops before the genuine cardholder realises his loss and cancels the card. The introduction of chip and PIN will make this more problematic, however, which will lead the criminal to seek new avenues for making purchases. CNP transactions generally only require purchasers to enter the details that appear on the face of the card, making them an easier target for fraudsters.

Indeed, for CNP transactions the fraudster does not even need to be in possession of a card at all. A criminal may fraudulently obtain the details of a genuine card, for example when a card is handed over for payment in a restaurant, while the cardholder is none the wiser.

A marketplace for fraudsters?

Fraudsters seek to buy easily exchangeable, high-value items which are desirable and easy to sell on. Electrical goods such as laptops, MP3 players and digital cameras are prime examples. The recent explosion in the popularity of online marketplaces, like eBay, means that criminals now have access to a worldwide market for their fraudulently obtained goods.

eBay states that about 0.01 per cent of transactions conducted on its sites are fraudulent, involving goods that were stolen, not as advertised or never delivered. But the genuine figure would be hard to assess, and could be considerably higher. Even taking the estimate of 0.01 per cent, with more than 300 million items listed on eBay in both the second and third quarters of 2004, 0.01 per cent of transactions would amount to well over 100,000 fraudulent transactions each year.[13] Criminals are rapidly turning eBay into one of the world's biggest fencing operations, and while eBay works hard to tackle these problems its sheer size makes it increasingly difficult to police.

Liability issues

From a liability point of view, the introduction of chip and PIN is significant. As of 1 January 2005, banks will no longer accept liability for fraudulent transactions where the use of chip and PIN could have prevented the fraud. The liability for these transactions will now fall on the retailer.

Merchants bear the liability risk

If a traditional retailer upgrades to a chip and PIN terminal then it will be protected against the cost of card fraud — whether a customer enters his or her PIN or signature — provided that onscreen prompts and routine checks are followed to ensure cards have not already been reported lost or stolen. Banks and card issuers will continue to be liable for the cost of card fraud committed on old-style non-chip-and-PIN cards. But liability shifts from the card issuer to the retailer where the retailer has not upgraded to chip and PIN and continues to accept a signature where a PIN could have been used.

This, of course, does not apply to CNP retailers, which have always traditionally picked up the bill for fraudulent transactions. Whereas regular retailers can upgrade to chip and PIN and benefit from card issuer protection, chip and PIN cannot be used on CNP transactions. CNP retailers will therefore continue to assume the risk and bear the full brunt of liability for fraud.

Chip and PIN therefore presents a double blow for CNP retailers. Not only do levels of CNP fraud look set to rise as chip and PIN displaces fraud from counterfeit and lost and stolen cards to CNP transactions, but CNP retailers also face the full cost of fraud as they are unable to benefit from card issuer liability.

Triple blow for CNP merchants

esult is that CNP retailers will end up suffering a triple blow, bearing the cost of loss of the goods, repaying the defrauded sums to the customer and meeting the card issuer's fees.

Alternative anti-fraud measures

If the protection of chip and PIN is unavailable, what can CNP retailers do to protect their position?

There are a number of basic checks which CNP retailers should be carrying out on any transaction. In 2001 the banking industry introduced the Address Verification Service (AVS) and Card Security Code (CSC). These methods verify additional information, supplied by the cardholder, in order to help the retailer to decide whether to proceed with the transaction.

Reducing the risks in CNP transactions

CSC provides additional security digits to confirm that the card number given is genuine — in the case of Mastercard, Visa and Switch this is the last three digits on the signature strip. AVS allows the retailer to confirm the numerics (ie the house or flat number and numbers from the postcode) in a cardholder's billing address with the card issuer. While a fraudster with a lost or stolen card may be able to supply a CSC, it is less likely that they will be able to provide the genuine cardholder's address as well.

If AVS is not used, personal address details can be checked in the electoral register, the telephone directory, with third-party suppliers or from BT's Phone Disc CD-ROM. Other checks might include contacting the customer by phone to confirm the order and checking that the delivery address has not been used previously with different card details. APACS has issued best practice guidelines for CNP retailers, including these and other suggestions.[14]

A variety of third-party service providers have produced solutions to help identify and prevent fraudulent transactions. Cyota's eSphinx system relies on transaction risk analysis software which assesses whether there is anything untoward with a banking customer's online activities. EarlyWarning's CardAware database provides an up-to-date list of high-fraud-risk cards. Other products are available, all of which help retailers assess the risk levels associated with a CNP transaction.

These methods will help to raise the authentication level in checking that the card user is who they say they are. But they will not do anything to alter the fundamental liability position which CNP retailers have for card fraud.

To help balance this position the card issuers have created online authentication schemes to improve online payment security. SecureCode from Mastercard and Verified by Visa use 3-D secure protocol technology to secure card transactions over the internet.

The systems work by creating a 'trust chain' throughout a transaction which verifies both the cardholder and retailer. The services allow cardholders to use personalised passwords to verify their identities when shopping online. The card issuer then authenticates the cardholder and notifies the retailer that the buyer is legitimate.

Most importantly for online retailers, enrolment in either SecureCode or Verified by Visa shifts fraud liability back to the card issuer.

3-D secure protocol technology clearly provides benefits to internet-based merchants. But it does not offer help to CNP retailers operating over the phone or otherwise. And the majority of online retailers continue to rely on basic fraud protection techniques, such as manual review, AVS and CSC checks. Only 23 per cent of online merchants are currently using Verified by Visa or SecureCode, although a further 43 per cent are planning to introduce the systems in 2005.[15] It will be interesting to see whether the implementation of such schemes can offset the expected increase in fraud caused by the introduction of chip and PIN, and encourage the development of similar schemes for other CNP retail channels.

References

1. APACS (2005) *Card Fraud the Facts 2005*, available at www.cardwatch.org.uk/images/uploads/publications.
2. *Ibid*.
3. *Ibid*.
4. *Ibid*.
5. *Ibid*.
6. *Ibid*.
7. *Ibid*.
8. Chip and PIN Programme Management Organisation (2005) press release, 29 March, available at www.chipandpin.co.uk/reflib/050324_Report_launch.pdf.
9. Anderson, R., Bond, M. and Murdoch, S.J. (2005) *Chip and Spin*, available at www.cl.cam.ac.uk/~mkb23/spin/spin.pdf.
10. APACS, ref. 1 above.
11. Jaques, R. (2004) 'UK tops European online shopping league', *Computing*, 11 November; Derbyshire, D. (2004) 'Retail sales are doubled on internet to £40bn', *Daily Telegraph*, 23 November.
12. APACS (2004) 'Spot and stop card-not-present fraud', available at www.cardwatch.org.uk/pdf_files/cnp_pack.pdf.
13. Altman, Daniel (2004) 'Is internet auctioneer an arena for criminals?', *International Herald Tribune*, 26 October.
14. APACS, ref. 12 above.
15. Cyber Source/Retail Logic (2005) 'UK online fraud report: Online payment fraud trends and merchant responses', available at www.retail-logic.com/Downloads/UK_Fraud_%20Report_2005.pdf.