Debit cards, ATMs and negligence of the bank and customer

By

Stephen Mason

This is a companion article to the following: 'Electronic banking and how courts approach the evidence', *Computer Law and Security Review*, Volume 29 Issue 2 (April 2013), 144 – 251

Key Points:

a) Customers continue to suffer losses when using debit card "chip and pin" technology at ATMs that they ascribe to the fault of the bank.
b) There are many instances where the bank uses its strength to ignore the failure of the security of its systems.
c) The provision of secure and reliable banking systems must be the cornerstone of any duty that a bank owes its customer – and judges ought to take a robust view in favour of the customer where a bank fails to provide this.

Abstract:

There is little or no guidance from the courts as to what constitutes the negligent use of bank debit cards. This article considers the negligence of both the bank and the customer in relation to debit cards and ATMs. A distinction is made between duties surrounding the use of the cheque with that of "chip & pin" technology.

The introduction of 'chip & pin' technology to debit and credit cards in the United Kingdom was aimed at reducing the theft of cash, mainly through Automated Teller

Machines (ATMs), by thieves that had worked out how to by-pass the security mechanisms put in place by the card issuers. This action was partly successful, although the figures have increased after a temporary reduction shortly after the introduction of the chip became effective. The rights and duties of the bank and the customer are generally determined by the terms and conditions that apply to the account, together with the provisions of the Payment Services Regulations 2009 (Statutory Instrument 2009 No. 209); this Statutory Instrument implements Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance) OJ L319, 5.12.2007, p. 1–36. In the main, the contractual and legislative position significantly overlaps with any action in negligence that either the customer or the bank might have against the other.

There is little or no guidance from the courts as to what constitutes the negligent use of bank debit cards, and this article considers the negligence of both the bank and the customer in relation to debit cards and ATMs. Consideration is given to the duties of the customer and the bank, and what type of action or failure to act might be considered to be negligent in each case.

When determining if either the customer or the bank is negligent, it is necessary to consider whether the customer or bank acted negligently or omitted to do something they should have done, and if so, whether the loss sustained was the natural result of the negligence of the customer or the bank, or their failure to act. Whether there will be an effective remedy in damages is not considered.

The duties of the customer

The customer's contractual duties clearly overlap with any duty they may have in negligence. It is certainly the case that the customer owes a duty to the bank when writing a cheque to take reasonable and ordinary precautions against forgery. It must also be right that the customer also has a duty to take reasonable and ordinary precautions to prevent their card from being stolen or used by a thief.

The duty to protect against forgery

With a cheque, the customer is required to take reasonable precautions against forgery. But with a card and electronic signature (such as the PIN – a PIN is a form of

electronic signature), it is difficult for the customer to prevent a thief from obtaining sufficient information from the legitimate card.

This means that if the bank insists on using technology that is inadequate or far from perfect, then the bank must take the consequences. The bank cannot take advantage of the weakness in the technology that customers are required to use; the flows of data through a number of third parties; the failure of employees that are responsible for the technology; and the failure to fully control the complex sub-contracting that takes place within the industry. The bank cannot complain of the consequences of their own default against customers who are misled by those very defaults of technology and the failure to obey operating manuals.

The distinction between the cheque, and the card and a PIN lies in the manner in which the two items are used and the ease by which a perfect forgery is possible with the card and a PIN. The customer has more control when writing out a cheque, but the crucial difference between the cheque and the card and the PIN is that the card and PIN can only be considered to be in the relative safe keeping of the customer, and when the card is used, it is exposed to the weaknesses of the technology.

The customer is at the mercy of unknown unknowns. It is the bank that is aware of many of these unknown unknowns because they are internal to the bank, but the banks are also prey to their own unknown unknowns, yet the sector refuses to acknowledge the weaknesses in the technology. Indeed, as the criminal cases noted below illustrate, there have been (and probably continue to be) significant failures in the technology used by the banks.

A further discussion in relation to the intervention of a crime is considered below under the rubric ‘where the intervention of an intervening crime causes loss’.

The PIN

The bank will include a number of contractual duties relating to the PIN in the contract with the customer that include the following:

To take all reasonable steps to keep the PIN secret at all times.

To take every care to stop anyone else using the PIN.

To destroy the piece of paper the bank sends with a record of the PIN.

Not to write the PIN on the card or anything else usually kept with the card.

Customers are at a disadvantage when using the technology. The first disadvantage is that the bank makes it a requirement that the customer must use the technology, so the customer rarely has a choice about accepting and using a card. Second, there are many methods that thieves can use to obtain the PIN, the information stored on the magnetic strip of the card without the knowledge of the customer, and the card itself, as noted below. By using the magnetic strip only, banks in countries such as the United States of America have demonstrated an unwillingness to take reasonable precautions to protect their customers by introducing a chip. While the addition of a chip is not guaranteed to prevent thieves, it does act as a more effective barrier.

For this reason, a judge will have to decide what the 'reasonable steps' are that a customer must take to keep the PIN secret, and what the customer must do to 'take every care' to prevent anyone else using the PIN. It is unlikely that there will be any defined set of guidance produced by judges, because the facts in each case are different.

The duty of the customer not to reveal the PIN

It must be right that where a customer gives out the PIN to another person, whether it is a family member or a thief, the customer will, depending on the facts, have acted negligently, and will be prevented from claiming that they were not negligent. If the customer is disabled or not able to use the card and PIN because of their age or some other infirmity, it is possible not to be considered negligent where the PIN is given to a third party that is authorised to act on behalf of the customer. In such circumstances, the bank should be made aware of such an arrangement, and be given information about the person with the authority to act for the customer. Where a third party acts on behalf of the customer, the duties that bind the customer will also bind the authorised third party.

When assessors at the Financial Ombudsman Service consider complaints, reliance is placed on the guidance set out in the *Electronic Funds Transfer Code of Conduct* (as revised by the Australian Securities and Investments Commission's EFT Working Group) (Issued 1 April 2001 Amended 18 March 2002 and 1 November 2008). Although a customer might not be aware of this Code of Conduct, there should not be a difference between what is covered in the Code and the terms and conditions of the bank.

In assessing whether a customer has contributed to losses by writing down the PIN or any other code, the following principles will apply, as set out in *Banking & Finance Policies and Procedures Manual (Extract dealing with Credit Card Disputes and Electronic Funds Transfer Investigations)* (Financial Ombudsman Service, 2008). These principles will also apply to any device used for on-line banking:

A user may keep a record of the PIN.

The PIN should not be written on the card.

The customer should make a reasonable attempt to protect the PIN.

If the PIN is not reasonably protected, it must not be carried with the card, or kept in such a way that it could be lost or stolen with the card.

Protecting the PIN comprises two aspects: that of disguising the PIN in a reasonable way, and taking reasonable steps to prevent the PIN from being obtained without authority.

Where a PIN or password is chosen by the customer, it is important to ensure that it is not easy to guess. For this reason, the Financial Ombudsman Service has indicated that a customer will usually be in breach of the principles where the customer decides on a PIN that represents their date of birth or is a part of their name that is easy to recognise.

Disguising the PIN

In *Banking & Finance Policies and Procedures Manual*, the Financial Ombudsman Service offer some advice as to what a customer can do to conceal or disguise the PIN or password. They include:

Re-arranging the numerals or letters that the bank has provided, and substituting other numbers, letters or symbols.

Concealing the PIN or password by:

making it appear as another type of number or word, or surrounding the PIN or password with other numerals, letters or symbols

placing the PIN or password in a location or context where it would not be expected to be found, such as on a piece of paper in a cookery book

using a combination of all of these approaches

Whether the disguise of the PIN is reasonable

Where a PIN or password has been disguised, the problem might be that the method used by the customer has not been effective. The Financial Ombudsman Service has indicated that the attempt to disguise the PIN does not have to be the most reasonable that could have been used. The method of disguising the PIN might not have been successful, but the lack of success does not make the attempt to disguise it unreasonable. How reasonable the disguise was will be considered on its merits, and each case must be taken individually.

In considering whether the attempt to disguise was reasonable, an assessment will be made from the point of the reasonable user that is a person:

- of average intelligence
- who does not have the knowledge and experience of a thief or bank claims officer about the strengths and weaknesses of different types of disguises
- who has sufficient, but not specialised, computer skills when it comes to using banking facilities
- who is aware of widely publicised warnings by their bank and the Ombudsman about unsafe methods to disguise a PIN

If a PIN is disguised in a way that a thief can easily find it, it is more likely that the customer will be considered to be negligent. Examples provided by the Ombudsman include:

- Recording the PIN as a series of numbers with any of them marked, circled or highlighted to indicate what the PIN is.
- Recording the PIN in such a way that it stands out as a PIN, for example where the PIN is recorded as a four digit ‘telephone number’ when all the other telephone numbers are eight digit numbers.
- Recording the PIN in isolation from other information.
- Recording the PIN as a birth date, postcode or telephone number without the benefit of a further element of disguise.

Ways in which a customer might be considered to be negligent

There has not been any case law in England & Wales to provide a list of examples

about what might be considered to be negligent, but a number of cases in Germany provide some guidance. The list below is from the German cases (taken from Assistant Professor DDr. Gerwin Haybäck, 'Civil law liability for unauthorized withdrawals at ATMs in Germany' *Digital Evidence and Electronic Signature Law Review*, 6 (2009) 57 – 66). It is possible that judges in England & Wales might reach different decisions because of different facts. Nevertheless customers might be considered to be negligent in the following circumstances:

(i) By keeping a written note of the PIN in an address book together with the card.

(ii) Where the customer places bank statements and the card carelessly into the pocket of a coat or jacket.

(iii) If the customer leaves their flat for three or four hours and leaves the card and the PIN on the desk in their flat, or if the customer keeps the card and the PIN in a folder.

(iv) Keeping the card with the PIN (as a four-digit telephone number) together in a solid strong box in a locked sick room in a hospital.

(v) Where a purse containing the customer's card is placed in a shopping trolley in a department store.

The customer is also urged to shield the reader of a terminal when they key in their PIN. The value of such shields (when provided) is doubtful, given the wide variety of terminal designs, the location of terminals and how easy it is for others to observe the customer typing in their PIN.

It must also be right that even though the customer has a contractual duty to inform the bank of any circumstances that lead them to think that their card or PIN has been compromised in any way, nevertheless, failing to alert the bank immediately that they are aware that something might be wrong must also be considered to be a negligent act of omission.

Where the intervention of an intervening crime causes loss

A customer is not negligent where a criminal act for which they are not responsible intervenes between them and any loss they might suffer. With respect to cards and

electronic signatures (PINs), this aspect has the greatest significance in the twenty-first century.

The negligence of the customer and the effect of an intervening act was the topic of discussion in *London Joint Stock Bank v Macmillan* [1918] AC 777, in which a clerk presented a cheque drawn in favour of the firm or bearer, in the sum of £2.0.0 to a partner for signature. The partner was in a rush, and signed the cheque. Only the amount in figures was filled in, not the amount in words. The clerk subsequently added the words 'one hundred and twenty pounds' in the space left for the words and added the figures '1' and '0' respectively each side of the figure '2'. The clerk subsequently presented the cheque for payment and was never seen again. The firm took action against the bank to recover the money, without success.

In his argument before the members of the House of Lords, Holman Gregory QC for Macmillan and Arthur, the respondents, indicated the issue at 785:

> 'If a customer by his act or omission misleads the bank, and loss is sustained as the natural result of that act or omission, the customer is responsible for that loss. It is not necessary to quarrel with that principle. That involves two questions of fact: 1. Was there a negligent act or omission by the customer? 2. Was the loss sustained as the natural result thereof?'

It was argued without success at 786 that 'It was not the form in which the drawer drew the cheque which misled the banker, but the intervening crime….' and 'At any rate, the intervention of a crime is an important factor in determining whether the customer has been guilty of negligence.'

Lord Finlay LC considered whether the intervention of a crime acts to make a forgery too remote, and in the case he was providing a judgment upon, he was correct. However, his comment, at 811, if considered in relation to cards and electronic signatures, has a significantly different meaning:

> 'Indeed, forgery is the very thing against which the customer is bound to take reasonable precautions.'

With a cheque, this indeed is the case. But with a card and electronic signature, the opposite must be the case. The customer is not in a position to take reasonable steps against forgery, unless they never use their card and electronic signature (and even this is risky, as the case of *United States v. Albert Gonzalez* (08-CR-10223**,** 09-CR-

10262, 09-CR-10382, http://www.justice.gov/usao/ma/news/IDTheft/gonzalez.html) illustrates, for the risks of a thief obtaining sufficient information to forge a card and electronic signature have been with us since the invention of the cards, and as the technology changes, so the methods of attack will continue to alter and adapt. In fact, Lord Finlay LC accepted, at 811, that:

> 'No one can be certain of preventing forgery, but it is a very simple thing in drawing a cheque to take reasonable and ordinary precautions against forgery.'

Arguably, Lord Finlay LC was correct in respect of a cheque, but could not envisage the technology that the banking industry was to initiate some fifty-five years after he made these comments. It is now very difficult for a customer to take reasonable and ordinary precautions against forgery – in many ways, the need for the banks to produce adequate evidence to prove the customer was the person at the ATM withdrawing the cash is even greater now than with previous methods of moving money, such as the cheque. The fact is, that the perfect forgery is possible with cards and electronic signatures. In fact, Lord Finlay LC observed, at 812, how the cheque in question in the case before the House of Lords appeared to be a perfect forgery:

> 'The examination of the facsimile of the cheque when filled up shows how impossible it was to detect the fraud.'

Thus it is with cards and electronic signatures as a matter of course. In this respect, Lord Finlay LC (at 796) quoted the remarks made by Cleasby B in the case of *The Guardians of Halifax Union v Wheelwright* (1873-74) 9 – 10 L.R.Exch. 183 at 192, which have a resonance to the modern world of banking technology as ever they did when he wrote them:

> 'a man cannot take advantage of his own wrong, a man cannot complain of the consequences of his own default, against a person who was misled by that default without any fault of his own'

This is also a point noted by Viscount Haldene, at 816:

> 'the banker as a mandatory has a right to insist on having his mandate in a form which does not leave room for misgiving as to what he is called on to do,'

Although this is a cheque case, nevertheless the discussions by their Lordships help to place the technology used by the banks into context. When dealing with different forms of technology, additional considerations must apply. The first question of fact remains, although the complexity of the technology does not necessarily make this an easy question to answer: 'Was there a negligent act or omission by the customer?' Where it is determined that the first question shows that there was a negligent act or omission by the customer, the second question follows: 'Was the loss sustained as the natural result thereof?'

The first point of discussion is whether 'the customer knows that a forged cheque is in circulation and neglects to notify the bank'. Consider the various possibilities in relation to the technology of modern cards:

(i) First, the customer is aware of, and authorises others to use their card and electronic signature. In such a case, the customer might give each person a right, under given circumstances, to use the card and electronic signature on behalf of the customer. Where the customer's bank is aware of such an arrangement in advance, it might be that the bank will issue a second card to the authorised party, and then any transactions carried out by the authorised party will be undertaken under the terms of agency as between the authorised party and the customer of the bank. In circumstances where the authorised person goes beyond the authority extended to them by the customer, the customer will take the loss. Where the arrangement is less formal, and the bank is not aware of such an arrangement, the risk lies with the customer for any misuse of the card until such time as the customer informs the bank and requests the cancellation of the card, for instance. In both cases, where a person is authorised directly or implicitly to use the card and electronic signature, and goes beyond the mandate (whether the mandate is formal or informal), then a crime is being committed. In these circumstances, whether the customer has been negligent will turn on the precise facts of each case. The customer issued a mandate, and it is for the customer to ensure the mandate is not breached – that is, unless the technical weaknesses are such that money is withdrawn from the customer's account and neither the customer nor the authorised users of the card are responsible for the loss.

(ii) Second, the customer deals with their card in such a way that they know others will be able to find and use the card, and third parties know the customer has also written the electronic signature on or near the card, or the electronic signature is a sequence of numbers that are so closely associated with the customer that the customer will always use this particular sequence, or it is notorious as to where the customer keeps their electronic signature.

(iii) Finally, the customer may have taken great care to provide for the safety of their card and electronic signature, but in despite of this, a third party, possibly a close relative, obtains the card and electronic signature. Depending on the circumstances, the customer is generally not held to be grossly negligent. (These scenarios and the consequences are similar to the seal cases, for which, see Stephen Mason, *Electronic Signatures in Law*, chapter 1).

Now compare this proposition with the technology of the chip and pin card and the position a customer might find themselves in: Where the customer has knowledge that their card might be compromised, the customer has a duty to notify the bank immediately. For the customer to be liable, it is necessary to establish how and when the customer might become aware that their card was compromised. However, a customer is rarely aware that a forged card is circulating amongst thieves until they receive their monthly statement, or they check their balance and find the account denuded, or they wish to use their banking facilities to discover there are no funds available. The technology imposed on customers by the banks is such that a forged card and a forged electronic signature can be used minutes after a successful cloning of the card, or after the magnetic stripe has been skimmed and the electronic signature observed.

In this respect, the comments of Lord Finlay LC, at 795 no longer remain quite as true in respect of card technology: ‘Of course the negligence must be in the transaction itself, that is, in the manner in which the cheque is drawn.’

A second point to consider is the comment that ‘the intervention of a crime is an important factor in determining whether the customer has been guilty of negligence.’ With respect to cards and electronic signatures, this aspect of the argument used by Holman Gregory QC has the greatest significance in the twenty-first century. The

distinction between the cheque, and the card and electronic signature lies in the manner in which the two items are used and the ease by which a perfect forgery is possible with the latter. Lord Finlay LC observed, at 809 that 'the manner in which the cheque is to be filled up is entirely in the hands of the customer'.

The crucial difference between the cheque and the card and electronic signature is that the card and electronic signature can only be considered to be in the relative safe keeping of the customer, and when the card is used, it is exposed to the weaknesses of the technology used by the banks. A card can apparently be 'swallowed' by an ATM, and a thief can persuade the customer to think the ATM has taken the card, and subsequently retrieve the card when the customer has left the scene. The thief can then have a cloned version operating in seconds on the streets of a city thousands of miles away. The banks require customers to use technology that is imperfect, although they may claim otherwise – indeed, they have consistently claimed otherwise for many years, and yet the technology they use is continually demonstrated to be at fault.

Where the thief obtains the card, or the data, or the PIN (or all of these) from the customer

It is relatively easy for a third party to obtain the electronic signature and the details of the account in the magnetic stripe of the card without the knowledge of the card holder, (as a starting point, the reader is directed to Ross J. Anderson, *Security Engineering* (2nd edn, Wiley, 2008)) and a thief can even obtain the original card by deception or by intercepting it as it is sent from the bank to the customer by post, together with the electronic signature. This is the first point of attack on the technology that the banks make their customers use. The customer cannot be responsible for failing to deal with such risks.

Often, it will not be known how the PIN was obtained, and it will be for the judge to determine, based on the evidence before her, whether the bank has proven its case that it was the customer. For instance, in 1980, Dorothy Judd discovered two withdrawals were made from her account by use of a cash card and PIN in the sum of US$800 (*Judd v Citibank*, N.Y.City Civ.Ct., 435 N.Y.S.2d 210). At the material time she was at her place of employment, and her employer corroborated her evidence by writing a letter to confirm her presence at her place of work. Citibank produced computer print-

outs setting out the details of the withdrawals in issue, the content of which was explained by the branch manager. It appears from the report that the bank merely asserted, by way of a statement in support, that the security measures in place to prevent the unauthorised use of cash cards was so stringent as to prevent the possibility of a PIN from being used other than by the person whose number it was. Marmarellis J indicated that the case turned on issues of evidence, burden and credibility. In his judgment, the learned judge referred to the lack of expert qualifications of the manager, but not the evidentiary foundations of the statement from the bank, in which the soundness of the security system in place was asserted. He determined the issue by considering whether the plaintiff had proven her case by a fair preponderance of the credible evidence. In this instance, the issue was whether to believe the person or the machine. In reaching a decision, Marmarellis, J referred to the 1977 Report to the Congress *EFT in the United States, Final Report of the National Commission on Electronic Fund Transfers* (National Commission on Electronic Fund Transfers, Washington, D.C., October 1977) and recommendation 5, which reads:

> 'If the depository institution denies the alleged error or its responsibility for the error or unauthorized use, the customer should have the burden of initiating any further proceeding, such as a lawsuit, to establish his right to have his account credited or recredited. Once a lawsuit has been initiated by a depositor, the depository institution has the burden to prove that there was no error or unauthorized use for which it was responsible.'

The learned judge commented that the recommendations of the Commission were not law, and looked forward to legislation dealing with the issue. (The Electronic Fund Transfer Act (15 U.S.C. 1693 was passed in 1978 and the Electronic Code of Federal Regulations, Part 205 – Electronic Fund Transfer (Regulation E) applies to cash cards.) He decided not to apply the recommendations of the Commission, but commented, at 212:

> '… this court is not prepared to go so far as to rule that where a credible witness is faced with the adverse "testimony" of a machine, he is as a matter of law faced also with an unmeetable burden of proof. It is too commonplace in our society that when faced with the choice of man or machine we readily accept the "word" of the machine every time. This, despite the tales of

> computer malfunctions that we hear daily. [The] defendant's own witness testified to physical malfunction of the very system in issue.'

Marmarellis J determined that the plaintiff proved her case 'by a fair preponderance of the credible evidence' and judgment was awarded in the amount of the loss plus interest and disbursements. Two further cases followed in 1981 (*Feldman v. Citibank, N.A.,; Pickman v. Citibank, N.A*, N.Y.City Civ.Ct., 443 N.Y.S.2d 43) but it was the case of *Ognibene v. Citibank, N.A.*, N.Y.City Civ.Ct., 446 N.Y.S.2d 845 that is of interest in the context of this article, in which the judge took judicial notice of news reports in the media of a number of methods used by thieves to steal money from ATMs, including where money was stolen by deceiving the customer into cooperating with the thief.

The case of *Ognibene* is a useful reminder that the customer cannot be responsible for failing to deal with such risks. It must be for the bank to prove that the customer was not the subject of such an attack.

Criminals also obtain the confidential data held on debit cards from unsuspecting individuals with the specific intention of transferring the data to false cards in order to use ATMs to withdraw funds. A variety of methods are employed to obtain sufficient information from a card to use it to steal money, such as copying the data stored on the magnetic stripe on a card as it is used in the ATM, where a small electronic camera is mounted above the key pad of the cash machine, so it records the PIN being used, and a card reader is placed over the legitimate slot for the card, and the data is read simultaneously by the false reader, as described in the following cases: England & Wales *R v Cenan (Sebastian)* [2004] ECWA Crim 3388; 2004 WL 3255240 (CA (Crim Div)), *R v Chirila (Remus Tenistocle)* [2005] 1 Cr.App.R.(S.) 92; [2004] EWCA Crim 2200, *R v Dabijia (Catalin Ionut)* [2005] EWCA Crim 318; 2005 WL 588736 (CA (Crim Div)); Canada: *R v Ciocata* [2004] A.J. No. 207; 2004 ABPC 39.

Another methodology is described in the Singapore case of *Public Prosecutor v Meng* [2006] SGDC 243 involving defendants of an organised syndicate based in West Malaysia. This enabled thieves to collect details on the card numbers and the PIN before producing cloned cards.

The wide availability of small card scanners enables a card to be skimmed, which enables the thief to produce a cloned version of the card, (as described in *R v Taj, R v*

Gardner, R v Samuel [2003] EWCA Crim 2633; 2003 WL 22257755, *R v Wong (Kok Kee)* [2004] EWCA Crim 1170; 2004 WL 1060608 (CA (Crim Div), *Attorney General's Reference No. 73 of 2003 (Umaharan Ranganathan)* [2004] 2 Cr.App.R.(S.) 62; [2004] EWCA Crim 183; 2004 WL 229130, *R v Din (Ameen)* [2005] 2 Cr.App.R.(S.) 40; [2004] EWCA Crim 3364; 2004 WL 3131381; for Canada see *R v Coman* [2004] A.J. No 383; 2004 ABPC 18, *R v Naqvi* [2005] A.J. No 1593; 2005 ABPC 339, *R v Mayer* 2006 ABPC 30 for Singapore see *Balasingam v Public Prosecutor* [2006] SGHC 228) especially in restaurants and retail outlets, although the attacker may obtain the PIN by just watching the victim type the numbers into a key pad before stealing the card when the opportunity arises, for which see the New Zealand case of *R v Telea* Court of Appeal, CA396/00, 4 December 2000, Keith, Blanchard and Tipping JJ. Other methods to obtain a PIN include the use of a mobile telephone to take photographs, or the video facility to capture the PIN being used on a key pad, or the use of x-ray film to trap the card in the ATM, so after the victim fails to recover their card, the thief quickly returns to the ATM and recovers the legitimate card, having obtained the PIN.

In any event, the crime can be lucrative. For instance, in *R v Mayer* 2006 ABCA 149 (CANLII); 2006 ABPC 30 a group of thieves stole over C$1m in undertaking such activities. Not all problems with ATMs are the result of attacks by criminals: the banks themselves may be put into a position where they are required to admit that they have problems, such as the failure for ATMs to balance, as in *Porter v Citibank N.A*., 123 Misc.2d 28, 472 N.Y.S.2D 582, where an employee of the bank admitted that, on average, the cash machines were out of balance once or twice a week. Also, simple attacks can be equally as effective, such as theft of the card and PIN before it reaches the customer, for which see in India, *Bharteeya v The State* 121(2005) DLT 369; 2005 (83) DRJ 299; and England & Wales: *R v Molcher (Andrew Alan)* [2006] EWCA Crim 1522; 2006 WL 2049662 (CA (Crim Div)).

The negligence of the bank

There are a variety of ways in which a bank can be considered to be negligent in undertaking its duties towards its customers, many of which are noted in the discussion above by implication. In broad terms, for the customer to raise the issue, it will be necessary to challenge the efficiency of the security mechanisms put in place by the bank or offer a credible alternative explanation for what happened.

The failure of the ATM and back end banking systems [Heading type B]

The customer relies upon the hardware and software put in place by the bank and any third parties contracted with the bank to provide services within the payment infrastructure. Even such an innocuous series of transactions involving an ATM may well involve an ATM owned by a third party and rented out to another party, the telephone line to the bank may be controlled by yet another party, who may be responsible for the security; a database link may well exist between VocaLink (VocaLink was created on 2 July 2007 from the combination of Voca and LINK Interchange Network) or some other third party, and a facilities management company may well be a link in the chain between VocaLink and the issuing bank. For this reason, the customer is totally reliant on the security, integrity and robust nature of the systems in place, together with the assessments of the systems, the results of internal audits, external audits, and audits by insurers. None of this information is made available to the customer, so the customer has to have complete trust in the integrity and reliability of such systems and the ability of the banks to identify and prevent insider fraud taking place. Note also the United States case of *United States v. Albert Gonzalez*, in which Gonzalez and others obtained unauthorised access to networks over wireless networks that processed and stored credit card and debit card transactions, and then obtained files containing data and encrypted PIN blocks. The importance of this case cannot be emphasised too much, bearing in mind that the PIN should never be released to anybody, yet this case demonstrates that some card issuers apparently seem to be treating the security of PINs somewhat indifferently.

An example of where it is probable that such a breakdown occurred is in a case before Seneka J of the Papua New Guinea District Court, *Roni v Kagure* [2004] PGDC 1; DC84 (1 January 2004). The learned judge found for Mathew Roni against the Bank of South Pacific. Mr Roni discovered the loss of his Save Card, and informed the bank immediately he knew of the loss. It was not in dispute that the bank put a stop to all withdrawals on 21 October 2002 at 10 am. It subsequently transpired that a number of transactions occurred after 10 am, and the bank looked to Mr Roni to compensate them for the withdrawals. The evidence demonstrated that a number of withdrawals took place simultaneously at different locations, as described by Seneka J:

> ‘How could the person who stole [the] complainant’s Save Card on 18/10/02 withdraw K1000.00 from Mt. Hagen by 06:04 am on 21/10/02 and another K1000.00 from Goroka at 6:16 am [on the] same date. Then within 1 ½ hours later in Goroka at Bintangor and Best Buy used the card for K884.05. At about 8:30 am [the] same date withdraw K1000.00 from BSP Mt. Hagen. Defendant has no explanation nor raised any to these transactions.’

In this instance, the learned judge reached the conclusion that the bank was negligent. The report of the case does not indicate whether the card was lost with the PIN, but two separate ATMs were used to obtain access to and remove cash from the same account in two separate physical locations at roughly the same time.

The problem with cases of this nature, is that the evidence provided by the banks tends to assert their systems are perfect, and therefore they are not at fault. That this line of reasoning is unreliable can be observed from the case of Maxwell Parsons, who used an MP3 player to obtain details of cards as they were used in free standing ATMs. He entered a plea of guilty at Minshull Street Crown Court in Manchester in November 2006 to possessing equipment to make a false instrument, deception and unlawful interception of a public telecommunication transmission. He was sentenced to 32 months in prison. He, together with others, stole up to £200,000 from free standing ATMs. Reports in the media explained how it worked (Russell Jenkins, ‘Hole-in-wall thief used MP3 player,’ *The Times*, 15 November 2006): The telephone line that connects the ATM to a BT line was disconnected, and a two-way adaptor inserted. The MP3 player was then placed between the ATM output cable and the telephone socket. The MP3 player recorded the tones sent over the telephone line, and the data was subsequently converted to readable numbers using a separate computer programme, and added to cloned cards, which in turn were used to steal by buying goods using the legitimate data. The police were made aware of the scheme by accident when they stopped Parsons for a motoring offence in London. They found a false bank card in his possession, and after searching his home in Manchester, they discovered technical equipment necessary to carry out the swindle, together with 26 bank cards, 18 of which were cloned. As this prosecution indicates, it is clearly beyond the ability of the customer to exercise any control over their PIN, whether the card and PIN remains in their possession or not.

Lax banking controls

Other problems highlight the significance of this issue, in that the banks themselves are also partly to blame for the failure of their systems. An example of the sloppy controls that can become apparent with respect to ATMs is illustrated in the case of *Patty v Commonwealth Bank of Australia* Industrial Relations Court of Australia VI-2542 of 1996; [2000] FCA 1072. In this instance, A$27,400 was stolen from an ATM machine. The police investigated the complaint made by the bank, but reached the conclusion that there was insufficient evidence to prosecute. (Compare this with *Windebank v Pryce* [2001] NTSC 45, where the investigation was woefully inadequate). The bank subsequently continued to investigate the theft, and eventually dismissed Mr Patty. Of relevance are the findings of fact by the Judicial Registrar, none of which were significantly challenged in the subsequent application to review the decision. The findings of fact illustrate the slack nature of the controls that can exist within a bank respecting the security of ATMs. First, it is helpful to describe how the ATMs were serviced. The learned Judicial Registrar described the system as follows (there are neither page numbers nor paragraph numbers in the internet version of this judgment):

> 'ATM machines are usually accessed by removing two combinations, a top combination known as the 'A' combination or lock and the bottom combination known as the 'B' combination or lock. ATM service teams usually comprise two officers. The teams are rostered to attend to operational faults out of hours and especially to attend to these faults at weekends. Machine malfunction is common. Many operational faults are fixed by ATM service teams. The usual procedure involves each member of the team being responsible for calculating and removing either the A or B combination on the ATM. Each team member is issued with a sealed envelope which contains numbers which allow for the calculation of either the A or B combination.'

The events that occurred before the theft, together with the nature of the controls put in place by the bank, are taken from the judgment and merit setting out in detail below to illustrate the nature of the problem and the issues that can arise:

> 'At 13.43.39.04 (i.e. at 1.43 pm) Centofanti logged on with the Voice Response Unit (VRU) in Sydney. He did this by telephone from the Collingwood Service Centre at 150 Smith Street. Very soon thereafter, the applicant contacted the Security Monitoring Centre (SMC) and advised that

the service team was in the branch and was about to deactivate the alarm system. There are log reports provided by SMC and Wormald Security Monitoring Service confirming these logging on calls.

Centofanti attempted to obtain the B combination for the ATM by using a touch phone and keying in his staff number and (supposedly) the bank branch number. At about 13.45.33.04 (i.e. at 1.45 pm) Centofanti keyed in an incorrect branch number and could not further access a series of numbers which, if obtained, and deducted from other numbers held by him in a sealed envelope, would have provided the correct combination for the B lock on the ATM machine.

At this stage, the applicant went downstairs. He has stated that he went downstairs to use the toilet. Meanwhile, Centofanti, having failed to obtain the B combination because of an invalid branch number, attempted to contact two other bank officers by phone with a view to obtaining the correct branch number and accessing it. He was unsuccessful in locating either bank officer and began searching desk drawers in the hope of locating the correct branch number. He located a grey key card wallet in the top drawer on the left hand side of a desk normally occupied by the second in charge of the bank. Centofanti described the wallet as ‘old and tatty’. Within the wallet, on a ‘Record of Account Details Card’, two series of numbers were written. He assumed that the numbers might have been the actual combinations of the A and B locks for the ATM. He was correct in the assumption that one series of numbers represented the A combination. Using these numbers he removed the A combination. Using the other series of numbers, he unsuccessfully tried to remove the B combination. The applicant had by then returned from downstairs. Centofanti asked the applicant to try and remove the B combination using the numbers on the card. The applicant tried and was also unsuccessful.

The Court pauses to note that the recording of ATM combination numbers and the leaving of such numbers in any place where access might be obtained was a clear breach of the respondent’s security procedures. This was only one of many breaches of security procedures which occurred at 150 Smith Street and which appear to have occurred frequently at many branches of the bank. On

that day Centofanti was responsible for the B combination. His removal of the A combination was a breach of security procedure. The applicant was responsible for the A combination. His attempts to remove the B combination were also a breach of security procedure.

At this stage, Centofanti successfully contacted another ATM service member by telephone and obtained from her the correct branch number. While Centofanti was so engaged, the applicant continued to search desk drawers in the hope of locating the B combination.

Once Centofanti had obtained the branch number he logged on again with VRU by touch phone and was placed on hold. At weekends, service team members often have to wait to be provided with numbers which allow calculation of combination locks. Such relatively short delays appear to be an inevitable result of the volume of telephone calls made by service team members. While Centofanti was on hold, the applicant successfully 'solved' the ATM 'communication problem' by resetting a controller or rebooting a modem.

While the applicant was so engaged, Centofanti obtained the appropriate numbers from VRU and calculated the B combination which he wrote on 'a piece of paper'. Although the ATM communication problem appeared solved because of the applicant's resetting of a controller, Centofanti decided to open the ATM and confirm the machine was working by performing what is known as a 'COCO' test. To perform the COCO test, having earlier removed the A combination, he removed the B combination using the combination number on the piece of paper, partially opened the ATM security door and flicked a toggle switch located inside the ATM security area. The ATM then performed a self test program which registered a 'COCO display' which indicated that the machine was once more in working order. Centofanti then secured the ATM door by spinning the combinations and telephoned VRU to log on for the next service call. At the same time, the applicant advised SMC that the alarm was about to be reactivated.'

The banks, by various mechanisms, force their customers to use technology, yet the very systems upon which they rely are not always as robust as they could be. As

Professor Anderson illustrates in his text, the systems put in place by banks are not as secure as some maintain. For instance, it was demonstrated that it was possible for an attacker in the bank to discover approximately 7,000 PINs relatively quickly (Mike Bond and Piotr Zieliński, 'Decimalisation table attacks for PIN cracking' Technical Report Number 560 (February 2003, Computer Laboratory UCAM-CL-TR-560)), and known weaknesses in standards that may be responsible for unauthorised withdrawals have not been addressed by the banks.

Additionally, the processing system used by banks is open to abuse. One method is to attack the translate function in switches, and another makes use of the functions that are used to allow customers to select a new PIN on-line. In both instances, the flaws enable an attacker, if they have access to the on-line PIN verification facility or switching processes, to discover PINs, such as those entered by customers while withdrawing cash from an ATM (for which, see Omer Berkman and Odelia Moshe Ostrovsky, 'The unbearable lightness of PIN cracking,' available on-line at http://www.arx.com/documents/The_Unbearable_Lightness_of_PIN_Cracking.pdf. For information about different types of attack on ATMs in the past, see Ann All, 'ATM History Industry 2002: A year in view' 7 January 2003 on-line at http://www.atmmarketplace.com/article.php?id=3281).

Insider theft

Thefts also take place entirely from within the bank, for which see *United States of America v Bonallo*, 858 F.2d 1427 (9th Cir. 1988); *Kumar v Westpac Banking Corporation* [2001] FJHC 159; *Sefo v R* [2004] TOSC 51 and *R v Clarke* [2005] QCA 483. See *Windebank v Pryce* [2001] NTSC 45 for a discussion of 'Night and Day' cards, and the inadequate safeguards in place within a bank branch respecting the PIN, and lax controls over logging on to computers by members of staff.

The problem is not always the failure of the bank ATM system, but in the procedural system employed to issue cards of a similar nature, such as electronic benefit transfer cards issued by the Retirement and Disability unit of the Penrith office of Centrelink described in *R v Thompson* [2002] NSWCCA 149), although attempts at stealing large sums of money tends to be conducted with help from a mixture of the slipshod controls within the bank itself, together with somebody working on the inside of the bank, as illustrated in the cases of *In the matter of Adeniyi Momodu Allison v Bow*

Street Magistrates' Court ex parte Adeniyi Momodu Allison, R v [1998] EWHC Admin 536, in which it was alleged that Joan Ojomo, a credit card analyst, supplied account information to her external co-conspirators, who were then able to obtain a PIN or replacement PIN to draw cash from ATMs, and *R v Stephen Edward Seaton* [1998] EWCA Crim 754, the details of which are described by the Vice President:

> 'The applicant and the others conspired to obtain money from automated teller machines, referred to as ATMs, by the use of counterfeit credit and cash cards. They planned to enter British Telecom exchanges with the assistance of corrupted employees of that organisation, in order to gain access to lines passing from ATMs to the mainframe computers. Taps and memory boards were placed on those lines, and used to record details of the cards of account holders while they were being transmitted down the lines. Those details recorded in that way were then to be downloaded onto a computer, and decrypted.
>
> The information obtained by that means was then to be transferred, using a read/write machine, onto blank plastic cards obtained for the purpose. The blank cards thus informed could then be used at ATMs to withdraw money.
>
> The applicant played a major role in this conspiracy. He had a list of door code keys for every telephone exchange within the M25 area, and he said those had been obtained from a BT engineer. The coaccused, Moore, was in charge of the computer program. The coaccused, Haward, owned premises which constituted the main operational base for the conspirators.'

In another case, that of *R v Stubbs* [2006] EWCA Crim 2312, a clerk, a member of a password reset team (comprising two people), was involved in fraudulent money transfers from the HSBC Bank between 23 July and 27 July 2002. In this case, four attempts were made to transfer money from corporate clients of the bank using an on-line banking system called 'Hexagon'. A fifth attempt, against the account of AT&T Wireless, succeeded. Three money transfers, each of about £1.9m, were made from the AT&T account on 25 July to an account held with Barclays Bank in Leicester in the name of Advanced New Technologies Corporation Ltd. The deposit was then converted into euros before being transferred to the account of a company registered in Spain, trading as Vasat Importacion SL in Madrid. A further transfer of £6.1m was

effected on 26 July from the AT&T account to the same recipients. None of the money removed from the AT&T account was recovered.

Note also the Canadian case of *R v Brum* [1999] O.J. No. 4727; [2001] O.J. No. 1731 in which the appellant was alleged to be in possession of both the upper and lower combination sets of access codes used to service ATMs, but the members of the Court of Appeal agreed that the evidence was not sufficient, and ordered a new trial.

The duties of the bank

A useful source of information that helps to reinforce the duties expected of the banks as set out in the Financial Services Authority book *Banking: Conduct of Business sourcebook*, is a guide written by the British Bankers' Association, the Building Societies Association and the Payments Council for its members in January 2011 with the title *Industry Guidance for FSA Banking Conduct of Business Sourcebook*. Although any rights that may accrue under the provisions of the *Banking: Conduct of Business sourcebook* and section 150 of the Financial Services and Markets Act 2000 might be narrowly defined, nevertheless it is arguable that the provisions set out in *Industry Guidance* ought to be considered in a wider context, given that the document recognises that banks have significant duties to perform. Two sections are particularly relevant, in the light of the comment in the introduction that states 'Firms regulated by the FSA must also comply with the FSA's Principles for Businesses'. The introduction to section 5 provides the following:

> 'Section 5: Post sale requirements
>
> 5.1 Introduction
>
> Chapter 5 of BCOBS sets out rules relating to the way in which a firm must treat a customer after they enter into a contract for a product or service. Firms must act promptly, fairly and efficiently when providing retail banking services.
>
> The way that firms deal with customers post sale is important in achieving the desired outcomes for Treating Customers Fairly under FSA's Principle 6. In particular firms should have regard to outcome 5:

"Consumers are provided with products that perform as firms have led them to expect, and the associated service is of an acceptable standard and as they have been led to expect."

As per Chapter 2 of BCOBS, all information provided to customers post sale must be fair, clear and not misleading.'

In this document, the industry has accepted the need to provide customers with proper advice and help.

What is interesting is what this document leaves out. It does not require the banks to conduct a fair, efficient, thorough and speedy investigation. It might be argued that a bank has failed to 'act promptly, fairly and efficiently' where employees have responded in an aggressive and unhelpful manner to a complaint relating to unauthorised transactions, and where the bank does not investigate a complaint, or does not investigate the complaint with any due diligence. Some of the factors that should be considered in deciding whether the bank has acted with diligence will include, but not be limited to:

(i) How swiftly the bank put a stop on all future transactions after being informed by the customer that they were not responsible for a number of transactions.

(ii) The speed at which the bank physically inspected any ATM or point of sale terminal.

(iii) The quality of the technical evidence, and whether the bank made any attempt to balance the technical evidence from their logs relating to the transactions in dispute against the transaction counter on the customer's card.

(iv) Whether the bank took any steps to secure any relevant cctv recordings.

The position on the security systems used by the banks when operating ATMs and on-line banking is considered by section 5.9 of the *Industry Guidance for FSA Banking Conduct of Business Sourcebook*, as agreed by the banks themselves:

'5.9 Account security

To provide a fair and efficient service firms must provide secure and reliable banking systems. Important aspects of this process include having effective systems in place to allow customers to report thefts or losses and making

available to customers useful information to help them protect their accounts. Such information could include:

- how to notify the firm promptly of any changes to the customer's personal information e.g. name, address and contact details;
- the benefits of checking statements and passbooks regularly and alerting the firm to any irregularities;
- how to keep cards, PINs, chequebooks, statements and security details safe; and
- how to alert the firm promptly to the loss of theft of any account details.

If using online banking:

- how to keep the customer's PC secure;
- how to keep passwords and PINS secret;
- the need to treat e-mails from senders claiming to be from the firm with caution and being wary of e-mails or calls asking for personal security details; and
- advising customers how to access internet banking sites by typing the bank or building society's address into the web browser i.e. not using a link in an e-mail.

Firms are encouraged to refer to the relevant rules at BCOBS 5.1.11 and 5.1.12 for details of a firm's and a customer's liabilities for unauthorised payments.'

The banks have accepted that they must 'provide secure and reliable banking systems.' Furthermore, the banks also accept that an important part of the process includes 'having effective systems in place to allow customers to report thefts or losses', but not, it seems, a fair, efficient, thorough and speedy investigation.

Chip and PIN technology has had an adverse effect on customers in two significant ways:

(i) When a correct PIN is entered, the bank assumes it is dealing with the customer, or a person authorised by the customer.

(ii) The systems used do not provide for different security mechanisms or settings for different types of use. This means a thief can obtain a PIN by

observing a low-level transaction, and can then use the PIN for a high-level transaction.

Part of the problem for the banks, and by implication for those customers that are affected by unauthorised transactions, relates to the assumptions noted in (i) above. This is highlighted by a comment in the report 'Checking out chip and PIN: The Northampton trial report 2003' (Chip and PIN Programme Management Organisation), in which the authors provide a list of questions and answers, one of which is as follows (on page 21):

> 'What is a PIN?
>
> A PIN (Personal Identification Number) is your 4-digit number which proves you are who you say you are. You tap in your PIN to verify a payment.'

This statement indicates a misunderstanding of what a PIN is and what it purports to do. The statement 'A PIN (Personal Identification Number) is your 4-digit number which proves you are who you say you are' is not correct. If this assertion was correct, then the fact that a transaction was carried out using the correct PIN would automatically mean it was the person to whom the card was issued who typed the PIN into a key pad. But a PIN is forged when it is keyed in by an unauthorised person, so the forgery obviously does *not* prove that the person who typed in the correct PIN is the person to whom the card was issued. The banks require customers to use a PIN in the full knowledge that when a PIN is forged, the issuer cannot tell the forged PIN from a PIN keyed in to an ATM by the customer. That the banks have chosen to use such a flimsy method of ascertaining their customers' agreement to a transaction with an ATM is their problem, and not the customer's – at least that is the legal position. But as any person who has had money removed from their account by a thief will be aware, making the bank understand that it was not the customer who withdrew the money can be far from easy.

A PIN on its own is not capable of proving you are who you say you are – in fact, a PIN even with some other form of link with your name (such as a credit card) is not capable of proving who you say you are. Both PINs and cards can be stolen and used by thieves without any fault on the part of their proper user.

Arguably, the PIN combines two functions. Before considering the two functions, consider the requirements of the bank. The bank needs to satisfy itself that the card is

legitimate, and the card is in the possession of the customer to whom it was issued, or a person authorised by the customer to use the card. For the bank to be satisfied of these two facts, a series of communications takes place for ATM transactions. In short, the chip or magnetic stripe on the card is interrogated by the ATM and back end systems, a method of verification takes place between the card and the system with the PIN, and the card is duly authenticated to the satisfaction of the bank.

The first function of a PIN is to act as a means of authentication. In this respect, all a PIN might demonstrate is that *the person that keyed in the PIN knows the correct PIN*. However, if the attack described by Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond in their article 'Chip and PIN is Broken' in *31st IEEE Symposium on Security and Privacy*, (IEEE Computer Society, 2010) pp 433 – 446 is used by the thief, then any PIN can be used, and the banking systems will register the PIN as being correct.

Once the computer systems of the card issuer are satisfied that the card is legitimate and the PIN is the correct PIN of the card holder, then the second function of a PIN enables the person at the ATM to undertake any activity on the account that is permitted within the mandate and within the limitations of the technology.

It must be right to say that the PIN, even though it is offered to the machine before a transaction is effected, acts as a signature to verify the customer's authority to make a payment or other form of transaction. In this respect, the presentation of a card to an ATM, and the input of a PIN can be likened to a cheque that is written out by the account holder, signed, and then presented to the cashier at the bank. The customer completes the action necessary to request a payment in advance of the payment being made by the cashier, and then signs the cheque in the presence of the cashier – all before receiving acknowledgement that a transaction has been authorised. In this respect, the PIN is a form of electronic signature.

It is certain that a bank ought to have the duty to provide 'secure and reliable banking systems'.

Concluding remarks

Banking systems that are wholly run by using technology are not perfect. Such systems will always be subject to being successfully undermined by thieves. However, the imperfections of the technology do not provide a reason for customers

to ignore the guidance issued by the authorities responsible for banking, or to fail to adhere to the contractual terms and conditions imposed by the banks. But even where a customer observes the guidance in full, it cannot be guaranteed that unauthorised transactions will not occur, especially as the result of the intervention of an intervening criminal act. In this respect, the provision of secure and reliable banking systems must be the cornerstone of any duty that a bank owes its customer, whether such duties are governed by negligence or a combination of contract and statute.

The only reason the weaknesses have been revealed in some instances, as discussed in this article, is because the banks were required to cooperate with the investigating authorities and explain and provide evidence of such weaknesses before the criminal courts. In civil actions, the banks have no incentive to reveal such weaknesses. The banks will deny that their systems suffer from any weaknesses, placing the blame squarely on the customer. It will be for the customer, should they ever have to consider taking legal action to recover money because of alleged unauthorised transactions that the bank will not reimburse, to point out to a judge that there is a series of cases that illustrate past weaknesses (some of which have yet to be remedied) that provide a good reason as to why the bank should be ordered to reveal, by way of example, any security evaluation performed on the bank's electronic banking system whether by its internal or external auditors, insurance inspectors, consultants or others supporting the claims of the bank that their system does not suffer from any weaknesses.

Unfortunately, not all banks respond well with complaints by customers, and if a matter gets as far as litigation, the banks tend to take an aggressive position in relation to the request by the customer, if such a request is ever made, for evidence that the bank has indeed put in place secure and reliable banking systems. It is for this reason that judges ought to take a robust view in favour of the customer. Even though the value of transactions that are the subject of theft that are acknowledged collectively by the banking sector is a tiny proportion of the value of the entire annual figure, nevertheless customers continue to suffer losses that they ascribe to the fault of the bank. It will be true to say that not every customer is right in their claim, but there are many instances where the bank uses its strength to ignore the failure of the security of its systems.

Stephen Mason is a barrister, specialising in digital evidence and electronic signatures. http://www.stephenmason.eu. With thanks to Nicholas Bohm for reviewing this article.