EDITORIAL

The use of information technology by the banking sector has not prevented criminals from stealing money from banks and organizations that issue plastic cards for the purposes of obtaining cash and buying goods and services on credit.

Digital evidence and electronic signatures may appear to be mundane – both to lawyers and lay people, but they affect everybody that has a bank account or uses a credit or debit card. The technology now used to deal with money cannot be considered to be ubiquitous across the globe yet, but the introduction of ATMs across many countries is now occurring at speed, especially in African states. The use of information technology by the banking sector has not prevented criminals from stealing money from banks and organizations that issue plastic cards for the purposes of obtaining cash and buying goods and services on credit. Indeed, criminals now have the capacity to steal far greater amounts of money than hitherto – they exchanged the horse for the motor car as a means of escaping from the scene of a robbery as soon as the technology permitted, and the more determined now manipulate customers through social engineering techniques, and take advantage of the flaws in the technology used by banks.

As the recent banking crisis has illustrated, many people in control of banks lost sight of what business they were in: risk (Samuel Johnson (taken from the edition improved by Henry John Todd, (John Walker, 1836)) defined 'bank' as 'a repository where money is occasionally lodged; to lay up money in a bank' and a banker as 'one who receives money in trust'). Banks deal with the risks inherent in the control of money, and in the increasingly complex world that humans have created, banks and how banks deal with the risks associated with the control and transfer of money affects everyone; indeed, governments *generally* take great care to oversee the mechanisms associated with the movements and stability of currency.

It is for this reason that customers of banks and governments ought to take as much interest in the systems used by banks to provide customers with a service (mainly through ATMs) as do criminals. In an attempt to reduce the ability of criminals to steal money from banks, the banks and card issuers have resorted to more technically complex methods (such as the adoption of EMV – that is, the inclusion of a chip on the card) of protecting the mechanisms (e.g. ATMs and Point of Sale terminals (PoS) that have become ubiquitous) used to dispense cash or permitting a customer to authorize transactions on their account. The problem with the increased complexity of the systems put in place by the banks, as the article by Dr Steven J. Murdoch illustrates, is that there is a corresponding increase in the risks associated with the flawed implementation of such systems.

In addition, the courts have not necessarily treated the delicate balance between the risks that should be borne by the banks and those risks the banks prefer to transfer to the customer. The decisions in the case of *29.06.2000, 2 Ob 133/99v* of the Oberste Gerichtshof (Supreme Court of Austria) and *Civil case No. 3K-3-390/2002* from the Lietuvos Aukščiausiasis Teismas (Supreme Court of Lithuania) represent a more realistic and accurate analysis of the position on legal liability than the judgment in the case of *5 October 2004, XI ZR 210/03* (published BGHZ 160, 308-321) by the Bundesgerichtshof (German Federal Court of Justice), each of which are translated into English and included in this edition of the Review.

In this respect, misunderstandings continue in relation to the technology and how the technology is analysed in legal terms. Consider, by way of example, the report 'Checking out chip and PIN: The Northampton trial report 2003' (Chip and PIN Programme Management Organisation).[1] In this report, the authors provide a list of questions and answers, one of which is set out below (on page 21):[2]

> What is 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.

Note the word 'verify' in relation to a payment usually means 'check that it has been made'. In this example, it seems 'verify' actually means 'authorize.' (Note that PINs can be between 4 and 12 digits; 5 digits are used in South Africa and 6 in France).

This statement indicates a misunderstanding of what a PIN is and what it purports to do.

In the same way that a manuscript signature can be forged, PINs are forged every day, as some customers of banks are aware.

If the assertion noted above were 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 can obviously be forged (that is, a thief can discover the correct PIN and then use it), so the forgery obviously does *not* prove that the person who typed in the correct PIN is the person to whom the card was

[1] *Available at hppt://www.chipandpin.co.uk/reflib/northampton_trial_report.pdf.*

[2] *The editor acknowledges the very helpful comments and suggestions made by Nicholas Bohm in respect of the discussion that follows.*

EDITORIAL

issued. The issuers of plastic cards 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 a machine by the actual customer. That the card issuers have chosen to use such a flimsy method of ascertaining their customers' agreement to a transaction with a machine 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 card issuer 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 the person is who they say they are – in fact, a PIN even with some other form of link with a 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 criminals without any fault on the part of their proper user.

The function of a PIN is to verify a payment

Arguably, the PIN combines two functions. Before considering the two functions, consider the requirements of the card issuer. The card issuer needs to know if the customer to whom the card has been issued is the person interacting with the ATM or PoS. If the bank or card issuer is satisfied on these two points, then the bank has satisfied itself that it is dealing either with the customer to whom the card was issued, or at least the card and PIN is in the possession of another person that has both the card and PIN with the authority of the customer.

Thus the bank or card issuer needs sufficient evidence 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 authorized by the customer to use the card). For the card issuer to be satisfied of these two facts, a sequence of events takes place for ATM transactions. They are summarized below.

Interrogation of the card

The first aim of the card issuer is to have sufficient evidence from the computer systems to demonstrate that the card issued to the customer is the card the computer systems are interacting with, and not a forged card. The ATM terminal interrogates the card to determine which technology it should use for the transaction (magnetic stripe or chip).

Verification of the card holder

The ATM prompts the customer to enter the PIN. The issuing bank compares the PIN to their records, and a message is sent back to the ATM to indicate whether the verification was successful. It does not follow that this process succeeds in all completed ATM transactions.

Authentication of the card

First, it should be noted that it does not follow that this process succeeds in all completed ATM transactions. With an EMV card (also called Chip & Pin in the UK), the chip will normally be interrogated to enable the issuer to determine whether the card is the one issued to the customer. If the chip is not read or cannot be read, the ATM will probably read the magnetic stripe on the card to perform a magnetic stripe fallback authentication, where the ATM sends the contents of the magnetic stripe to the issuing bank, via the card scheme network. The issuing bank will then verify whether it contains the correct information. Providing the bank or card issuer received satisfactory responses from either the chip or the magnetic stripe, and the PIN is correct, then the person at the machine is then free to undertake transactions on the account.

The functions of a PIN

Thus the functions of a PIN can now be analyzed. The first function of the PIN is to act as a means of authentication. In this respect, a PIN demonstrates that *the person that keyed in the PIN knows the correct PIN*.

The second function of a PIN is to act as a form of electronic signature. Once the computer systems of the bank or card issuer are satisfied that the card is legitimate and the PIN is the correct PIN of the card holder, then the person at the ATM or PoS can 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 authorized. In this respect, the PIN is a form of electronic signature.

Arguably, the legal analysis is relatively straight forward. The more difficult issue is to force the bank or card issuer to adduce the digital evidence, and then for the lawyer to test it effectively by cross-examination.

