Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

Banking and fraud

Stephen Mason [a,*], *Nicholas Bohm* [b]

[a] *Chambers of Stephen Mason, UK*

[b] *Foundation for Information Policy Research, UK*

Keywords:
Banking
Fraud
ATMs
Proof
Trust
Policing

A B S T R A C T

The authors wrote a memorandum to the UK Treasury Committee, House of Commons in January 2011 on the topic of banking and fraud. The methods used by thieves to steal from the customers of banks have increased, and in September 2016, the UK consumer magazine *Which?* made a super-complaint to the Payment Systems Regulator to (i) formally investigate the scale of bank-transfer fraud and how much it is costing consumers to take action, and (ii) propose new measures and greater liability for banks to ensure consumers are better protected when they have been tricked into making a bank transfer. This comment replicates the Memorandum submitted to the Treasury Committee on the basis of having our observations put on the record. The references have been updated and citations added. Apart from the increased variety of methods used by thieves to steal money, the remarks we made in 2011 remain true today.

The contemporary use of electronic machines by banks is so widespread, that it is difficult to imagine that the banking system would continue to work at all if such machines were withdrawn. But reliance on electronic machines carries with it hidden risks. There is an important but neglected distinction between purely mechanical machines, such as the first machines produced in the nineteenth century to dispense cigarettes, etc, and modern machines that rely on software, such as cash dispensers ('ATMs'). Software has approximately 5 defects per 1000 line of code. Given that most machines that rely on software have millions of lines of code, most commercially produced software products will have thousands of undetected defects. This is why software vendors have to issue updates to software (quite apart from the making of improvements). Such updates are correctly described as 'security updates', because some defects can be manipulated by a thief, for instance, for fraudulent purposes. Errors in the construction of purely mechanical machines are apt to make them fail in obvious ways; but software introduces such an enormous increase in complexity as to result in errors whose consequences are very hard to detect.[1]

The following is offered by way of example. A person authorized to enter a building may be issued with a token (often a plastic card with a magnetic stripe or a chip). To gain entry to the building, the user must swipe the card in a reader, insert the chip part into a reader, or press the card against the surface

http://www.stephenmason.eu

* *Corresponding author.* Chambers of Stephen Mason, UK.

E-mail address: stephenmason@stephenmason.eu (S. Mason).

[1] For references for the points made here, and for a more detailed treatment of this topic, see Stephen Mason, *Electronic Evidence*, (3rd edn, LexisNexis Butterworths, 2012) Chapter 5 and the references contained therein.

http://dx.doi.org/10.1016/j.clsr.2016.11.018

0267-3649/

Please cite this article in press as: Stephen Mason, Nicholas Bohm, Banking and fraud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.018

of a reader located on a wall or door. They may also be required to insert a code. Given this technology, it is taken for granted that the communications between the various items of software prove that (i) the card is physically present, and (ii) that the person to whom the card was issued is the person who enters the building. This assumption can be corroborated by evidence that they used various machines (mainly computers) in the building for a number of hours before leaving. Whilst the evidence that the authorized user used a computer is not conclusive that the person was either physically in the building or used the machine, nevertheless there would be strong circumstantial evidence to indicate they were present in the building from the moment the card was swiped in the reader.

However, machines run by software and controlled by a bigger machine that is linked to all the machines in the building (controlling computers, readers on different doors, cctv, air conditioning systems, etc) are also often linked to the internet. If the machine and the networked machines are linked to the internet, it is possible that a third person from another country (for instance) might gain access to the system remotely by taking advantage of defects in the system's software and might manipulate the system to make it appear that a person has entered (or left) when they have not.

The point is this: the fact that the software on a reader adjacent to a door is recorded as having communicated with the software in the central computer to send a message that a particular card has been pressed or inserted into the reader does not prove that (i) the person whose card it was issued to was in physical possession of the card, nor (ii) that the card was physically present against the card reader to cause the software to send the message to begin with.

Contemporary banking systems operate on the basis of an association of links (some of which are very flimsy) that the banks themselves use to assume that either (i) their customer, or (ii) another person with the authorization of the customer, is at the ATM or a computer terminal when undertaking an on-line transaction. A bank can never know if their customer is the actual person at the ATM or computer terminal.[2] The bank *assumes* that the customer is at the ATM if (i) the software in their system communicates with the software linked to an ATM, that (ii) a card is apparently physically present in the ATM, and (iii) the software on the card communicates with the software in the ATM in an attempt to verify that the card is a genuine card, and (iv) the personal identity number (PIN) (one form of electronic signature[3]) if correct, is that of the customer. Banks use the evidence thus accrued to assess automatically whether to allow the transaction to take place. The problem is that banking systems are not perfect, and can be manipulated, but representatives from the banks and banking industry are on record as claiming over the previous 40 years that their systems are safe and cannot be broken into by malicious outsiders, only for each new item of technology that is introduced by the banking sector to be proven to be open to successful attack.

1. The law

When a customer claims that money has been withdrawn from their bank account without their authorization, the legal issue is straightforward: whether the bank had the authority under its mandate from the customer to debit the account. Where a customer carries out a transaction at an ATM, for instance, the mandate will be fulfilled if the card issued to the customer and the correct PIN are entered in the machine by the customer. It is a primary issue whether the bank can prove that the customer or a person authorized by the customer authorized the withdrawal of the money, or that the carelessness or gross negligence of the customer enabled an unauthorized person to do so (where the mandate authorizes a debit on that basis).

1.1. *The burden of proof*

It is often suggested in the media that the burden of proof is on the customer to prove they did not withdraw the money. This is not correct. This has never been the legal position.

Prior to the Payment Services Directive and Payment Services Regulations 2009 (*SI 2009/209*) ('PSR'), it was for the bank, where it relied on the signature of the customer, to prove the signature was that of the customer if the customer did not accept the signature as their own. As a PIN is one form of electronic signature, the burden of proof has remained with the bank at all times. Under the new law, it is now for the bank to prove on the balance of probabilities that the card issued to the customer was inserted into the ATM by the customer or by a third party with their authority, and that the PIN was entered by the customer or by a third party with their authority. Article 59(1) of the Payment Services Directive[4] (regulation 60 of the PSR) provides that where a user denies effecting or authorizing a transaction, it is for the bank to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts, and not affected by a technical breakdown or some other deficiency.

1.2. *Evidence*

In the case of *Job v Halifax PLC* (not reported) Case number 7BQ00307,[5] Mason argued on Mr Job's behalf that the bank had

[2] Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity between Humans and Software Code, or whether You Know It Is a Dog, and if so, which Dog?' *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 5, 135–148.

[3] For electronic signatures, see Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016); *Lorna Brazell, Electronic Signatures and Identities Law and Regulation*, (2nd edn, Sweet & Maxwell, 2008).

[4] 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 L 319, 5.12.2007, p. 1–36.

[5] The judgment is reproduced in full in the *Digital Evidence and Electronic Signature Law Review* 6 (2009) 235–245.

Please cite this article in press as: Stephen Mason, Nicholas Bohm, Banking and fraud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.018

to produce evidence of the trail of communications between the various items of software associated with the transactions in dispute. The learned county court judge rejected this. However, the position has changed, and where the customer does not accept they authorized the transaction, article 59(2) of the Payment Services Directive (regulation 60 of the PSR) provides that the use of a payment instrument (that is, the card issued to the customer by the bank) is not in itself necessarily sufficient proof either that: (i) the transaction was authorized by the customer, or (ii) that the customer acted fraudulently, or (iii) the customer failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.

Regulation 60 of the Payment Services Regulations now provides that it is for the bank to provide a complete chain of evidence to prove their case: beginning with the records of the ATM, any communications systems used between the ATM and the bank back-end systems, and the processing of the data in the bank's systems.[6] So much the better; but the introduction of these more detailed requirements will still not be sufficient to protect the customers of the banks, however, if the general rule continues to be applied that machines may be assumed to work correctly. Such a rule effectively negates the requirement for evidence that systems are in fact working correctly, thereby ignoring the vulnerability of commercial software.

1.3. *The card*

One problem relating to the nature of the evidence is the card issued to the customer by the bank. The customer is almost always told by an employee or agent of the bank to destroy the card when the customer has cause to make a complaint. The card includes an Application Transaction Counter ('ATC'). The ATC is increased by one each time a transaction takes place. A test of the card will help to determine whether the ATC has been increased, and the test can enable a comparison of the transactions recorded on the customer's statements to establish whether there are any discrepancies. This is important evidence, and can help demonstrate whether the customer is telling the truth when they assert that they were not responsible for the disputed transaction. As a direct result of the bank telling the customer to destroy their card, the bank deliberately requests the destruction of evidence, knowing that legal proceedings may be taken by the customer to recover the money. For this reason, a bank can be held in contempt of court where such advice is given and acted upon. That banks issue such instructions to the customer is of utmost concern, because many customers destroy their cards when given such instructions by their bank, only to learn much later that the information on the card could have demonstrated that they were telling the truth.

[6] This is in line with the list of evidence set out by the Supreme Court of Lithuania in the case of Ž.Š. v Lietuvos taupomasis bankas, Civil case No. 3K-3-390/2002, Supreme Court of Lithuania, translated by Sergejs Trofimovs, *Digital Evidence and Electronic Signature Law Review* 6 (2009), 255–262.

2. The reporting regime

Since April 2007 (Home Office Counting Rules for Recorded Crime, Fraud and Forgery), consumers have been compelled to report fraud to their bank, and not to the police. If the bank determines that the customer was responsible for the withdrawal (or somebody authorized by them, or they were negligent), then the bank will not reimburse the customer. The customer can then complain to the police, but all the police will invariably do is give the customer a crime report number, and refuse to take any further action.

The reasons why the police do not tend to take action seem to be: (i) the high number of cases reported, (ii) the time, expense and expertise necessary to follow up such a complaint, and (iii) the apparently low importance attached to such crimes.

3. The reaction of the banks to the customer

When a customer complains to a bank about unauthorized withdrawals, some banks act with commendable speed and within the law. The legal position is set out by regulation 61 of the PSR, that is (subject to regulations 59 and 60) the bank must immediately refund the amount of the unauthorized payment transaction to the customer, and where applicable, restore the account to the state it would have been in had the unauthorized payment transaction not taken place. Unfortunately, there are a number of banks which do not comply with this requirement, and undertake what they call an 'investigation', only to inform the customer that as far as the bank is concerned, the withdrawal was carried out by the customer. The customer then in practice has to gather evidence to prove they were *not* responsible for the transaction.

4. Financial Ombudsman Service

It appears from the evidence that we have seen of how complaints are adjudicated by the Financial Ombudsman Service by people that have had money stolen from their accounts, that employees working for this authority have no understanding of the technical issues relating to digital evidence, nor do they appear to understand that it is for the bank to prove it did not let a thief steal its customer's money. Even when evidence from witnesses is put forward by the customer to demonstrate that they were not in the vicinity of an ATM when money was withdrawn, adjudicators at the Financial Ombudsman Service continue to accept the evidence provided by the bank. Often the bank will merely assert that because they claim the chip was read, it therefore follows that the customer was responsible for taking the money. It seems that adjudicators at the Financial Ombudsman Service tend to agree with the banks. The Service does not obtain evidence from the bank about the transaction in question to enable the customer to submit it to an appropriate expert for evaluation. It provides an inadequate protection for bank customers with disputed transactions.

Please cite this article in press as: Stephen Mason, Nicholas Bohm, Banking and fraud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.018

5. In our view, the following action should be considered if this issue is to be taken seriously

The government must change the rules for reporting and dealing with theft from banks accounts (either via ATMs or online), and for providing accurate figures for theft and fraud. At present, the only figures given for losses are those provided by Financial Fraud Action UK (previously UK Payments Administration Limited). These figures are not very clear and lack transparency. For instance, where a bank declines to refund a customer, the money in dispute is not considered by the bank as a loss, which means the loss is not reported to Financial Fraud Action UK, and is not included in the overall figures produced by this agency. The amount of money that might be in dispute may be considerable, and the figures given by the Financial Fraud Action UK are highly likely to be inaccurate for this reason.[7]

Police forces must have more funding to train police officers in digital criminal activities. It is crucial for the authorities to acknowledge that education, training and the provision of appropriate information technology to the police in respect of these crimes is essential. The failure to understand this fundamental point in the twenty-first century means that criminals will continue to be successful in stealing money.

The banks must put more robust methods in place to provide for the security of customers' accounts. They will not do so without the necessary incentive; and while they can pass the loss to their customers, they lack that incentive. The authorities appear to regard banking security as a matter for the banks. This approach worked well enough when a bank robbery meant that the bank lost money: it is up to the bank to decide how much to spend to protect itself from loss.[8] But modern banking is different: now bank robberies are electronic, and banks can protect themselves from loss by allowing it to fall on their customers by relying on the willingness of the law to presume that their systems are working correctly. In these new circumstances, banks can no longer be the judges of how to prevent fraud, because it is not them but their customers who carry the risk. This places wholly new demands on the competence of bank regulators, and it is not clear either that they recognize this or that they possess the necessary skills.

Consideration must be given to the general rule that machines may be assumed to work correctly. This rule ignores the susceptibility of commercial software to being manipulated successfully to the detriment of the customer.[9]

6. Further comments

Crime relating to bank accounts is complex. Unfortunately, the banking sector and police are, in general terms, treating this problem simplistically.[10]

Some indication of the scale and importance of the issue can be derived from the case of *R v Bunu*. It was heard at Hull Crown Court in July 2008. Not guilty pleas were entered and a 5–6 day trial ensued. The accused was found guilty of conspiracy. Media reports indicate that when he was arrested, police officers recovered details of more than 1900 accounts (some on a laptop), eight false cash point fronts, detailed lists of supermarkets around the country, card-cloning devices and between £3000 and £4000 in cash. The fingerprints of the accused were found on tape used to stick the false fronts on cash machines. It was estimated that about £43,000 was stolen, but it could have around £1.1m if they had used all of the 2000 sets of details they had obtained. In four months, two thieves obtained details from more than 2000 victims and cloned them on to loyalty cards, writing the PINs on the signature strips. They then travelled around the country to withdraw up to £500 a time with each card and using different cash points to avoid detection.[11]

Apart from the importance of this case as a demonstration of how easy it is for criminals to steal from banks using ATMs, there is a more telling point. In discussing the case after the conviction and sentence with one of the lawyers, it became clear that there was no indication by the banks or the prosecution as to whether each of the customers whose account details had been obtained by the thieves had been informed that their accounts had been compromised. Conceivably, customers might have had money stolen from their account by way of ATMs, but the banks might have asserted that it must have been the customer who made the withdrawals, even though it might have been because of the actions of Bunu and his accomplices. In this respect, it ought to be a requirement for the crown or the police or the banks, or all of these agencies, to inform the customers that their accounts have been compromised (unless this occurs in any event).

[7] Roger Porkess and Stephen Mason, 'Looking at debit and credit card fraud', *Teaching Statistics*, Volume 34, Number 3, Autumn 2012, 87–91 (This article was awarded the G Oswald George prize for 2012). For a translation into German, see Betrug mit Kundenkarten und Kreditkarten, Stochastik in der Schule 34 (2014) 2, S. 15–18).

[8] Banks and their customers are debtors and creditors. Although it is commonplace to speak of 'my money in the bank', and indeed hallowed by the Companies Acts to include an entry in a company's accounts for 'cash at bank', the cash actually held by a bank belongs to the bank, not its customers. The customers' only assets are their debt claims against the bank (if their accounts are in fact in credit). So when cash is stolen from a bank, it is the bank's cash, and the bank suffers the loss – the customers are not affected (unless the loss brings down the bank, of course).

[9] Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay', [2014] 30 *Computer Law and Security Review* Issue 1 (February 2014), 80–84.

[10] Maryke Silalahi Nuth, 'Unauthorized use of bank cards with or without the PIN: a lost case for the customer?' *Digital Evidence and Electronic Signature Law Review* 9 (2012) 95–101.

[11] This case was not reported, and the media reports of this case no longer appear to be live. For reports of similar reported cases, see Stephen Mason, 'Electronic banking and how courts approach the evidence', [2013] 29 *Computer Law and Security Review*, Issue 2 (April 2013), 144–151.

Please cite this article in press as: Stephen Mason, Nicholas Bohm, Banking and fraud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.018

Author Information

Stephen Mason is a barrister and the author of *When Bank Systems Fail – Debit Cards, Credit Cards, ATMs, Mobile and Online Banking: Your Rights and What to Do When Things Go Wrong* (2nd edn, PP Publishing, 2014).

Open access book: *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016) http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures.

Open access journal: *Digital Evidence and Electronic Signature Law Review* http://journals.sas.ac.uk/deeslr/ (also available in the LexisNexis and HeinOnline electronic databases).

Nicholas Bohm is a retired solicitor, formerly a partner in a major city of London law firm, and a trustee of the Foundation for Information Policy Research.

Please cite this article in press as: Stephen Mason, Nicholas Bohm, Banking and fraud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.018