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

ABSTRACT

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widespread, that it is difficult to imagine that the banking system would continue to work at all if such machines were withdrawn.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/© 2016 Stephen Mason and Nicholas Bohm

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.