CASE JUDGMENT: ENGLAND & WALES

CASE CITATION:
Job v Halifax PLC (not reported) Case number 7BQ00307

NAME OF COURT:
Nottingham County Court

JUDGE: **His Honour Judge Inglis**

DATE OF TRIAL: **30 April 2009**

DATE OF JUDGMENT: **4 June 2009**

COUNSEL FOR THE CLAIMANT:
Stephen Mason, instructed by the Bar Pro Bono Unit

COUNSEL FOR THE DEFENDANTS:
Adam Kramer, instructed by Cobbetts LLP, Leeds

ATM; electronic signature (PIN); proof for civil proceedings

Judgment

1. In this case Mr Job claims from Halifax PLC £2100 plus interest which he says the bank has wrongfully debited from his current account with them. The bank admit the debits, but say that they were justified because that money was withdrawn from the Claimant's account with them by use, at ATM's, of his card and the correct PIN.

2. History. The Claimant came from Cameroon to this country in 2000. His family, 2 daughters and his wife, came in about the same year. He has claimed asylum, but his application has not yet been finally determined, though he has temporary leave to remain and is not allowed to work. In September 2000 the Claimant opened a current account with the bank. The nature of the card issued for use with the account changed, but at the material time, in February and March 2006, it was a Visa Electron card which could be used, subject to there being sufficient funds in the account, for online point of sale transactions and for withdrawals at ATM's. The account was frequently used by the Claimant. Although he did not have income from earnings, he received support in particular from his cousin, who is a professional footballer. On 15 December 2005 the account was replenished by payment in of £10,000, which the Claimant says came from his cousin, and it remained healthily in credit until the events with which this case is concerned.

3. On 21 February 2006 the account had a credit balance of £3,565.59. There then followed, over an 8 day period, 8 debits reflecting, on the bank's case, use of the card. The withdrawals took place at 2 ATM's: HSBC Whitley Street, Reading, and Natwest 103, Basingstoke Road, Reading. Both ATM's are close to the address at which the Claimant was then residing, and both had been used by the Claimant in the recent past:

(i)	Wed 22 February 2006	1331	£300	HSBC
(ii)	Thur 23 February 2006	2127	£200	HSBC
(iii)	Thur 23 February 2006	2127	£100	HSBC
(iv)	Fri 24 February 2006	0026	£300	Natwest
(v)	Sun 26 February 2006	0936	£300	HSBC
(vi)	Mon 27 February 2006	1916	£300	HSBC
(vii)	Tue 28 February 2006	2112	£300	Natwest
(viii)	Wed 1 March 2006	2250	£300	HSBC

4. The Claimant's account of matters and subsequent events The Claimant says that the card was in his possession at all times, including during the period of the disputed transactions. He never told anyone else about his bank details, including the PIN number: neither his wife and 2 daughters nor anyone else. He has not authorised anyone else to withdraw money or given them the means of doing so. On the occasions of the withdrawals on 23 and 28 February he was coaching, or had just finished coaching, a football team. On 26 February he was on his way to or at a junior team football match. On 24 February he was at home. On 1 March he was at home watching television On that day in the evening he was at Morrisons waiting for his daughter to do her shopping. He decided to check the balance on his account at the ATM there. He did, and noticed "some irregular withdrawals from my account that I did not recognise". At the hearing the question was not resolved whether he had the ability at the ATM to call up a mini statement or only

the balance. At all events, he says he became aware that there was much less in his account than there should be. He did not ring the bank that night, believing that the office would be closed, but went home and watched television. Before he went to bed he took the card from his wallet and hid it under a griddle drum in the garden, retrieving it the next morning. The last questioned withdrawal took place after he had discovered the state of his bank account and while he was at home watching television, with his family in the house.

5. The next morning the Claimant went to the bank. He pointed out the withdrawals and was advised to inform the police. In the succeeding days he was sent another card. As the bank were prepared to accept, he did not receive it, and withdrawals made using it were refunded. On 10 April he was in the branch pursuing his complaint. He said he would not leave until he was re-imbursed. The police were called to see him off the premises. Halifax then closed the account. Re-imbursement was later refused, and the Claimant's complaint to the financial services ombudsman was unsuccessful. He begun this claim on 20 March 2007. The Claimant himself gave evidence in support of his account. There were statements from each of his daughters, who are now at university. The Claimant's wife, who was the other family member generally present at the material time, sadly died in 2008.

6. The Defence sets out the Defendants' case: that the Claimants card and the correct PIN were used for these withdrawals, and that (in its essentials) the transactions were either carried out by him, or authorised by him, or resulted from his gross negligence in enabling someone else to have possession of the card or PIN. Since it is the Claimant's case that he was in possession of the card at all times and had never divulged or compromised the security of the PIN, then if the bank proves that these transactions were made and that system error or third party fraud unconnected with the Claimant can be ruled out on the balance of probabilities, it is accepted the Claimant's case would fail.

7. The factual evidence for the bank consists of a printout of data resulting from interrogation of the computer system, which evidence these transactions. The printouts are not readily intelligible to the layman, and for their interpretation and other technical explanations the Defendants relied on the evidence of Ian Brown, Senior Consultant, Cryptographic services, HBOS group IT. There was also independent expert evidence: For the Claimant from Dr Steven Murdoch, a researcher in the security group at Cambridge University, and a fellow of Christ's college; and for the Defendants from Mr David Baker the head of APACS Cards technical unit, with responsibility for providing technical and operational oversight of the UK card payments infrastructure. APACS is a trade association of UK member banks.

8. The Claimant's card was a chip and PIN card. The Defendants' case is that, as used in these transactions, the CHIP on the card was used to interact with the bank's systems and so authorise the payments. The chip holds information, but it also contains a CPU, and so is also a computer. The card and the chip go after manufacture to a personalisation bureau. The chip is cryptographically unlocked and programmed as a Visa Electron chip. It is then locked again. Later the personalisation file is sent from HBOS to the personalisation bureau, doubly encrypted. Personalisation takes place during a production run using a combination of secret keys. The PIN is not processed by the card, but has to be used with it in order for a transaction to be authorised. When the card is used, the encrypted PIN is transmitted to and verified by HBOS systems.

9. Apart from the PIN, an ATM transaction involves what in laymens' terms could be described as a conversation between the chip on the card and the HBOS systems. They include cryptographic checks. During this process the chip, on request from the ATM, will produce an Application Request Cryptogram (ARQC). The ARQC will be generated using cryptographic keys on the card. In response HBOS systems will transmit an authorisation response Cryptogram (ARPC) which includes a decision on the request. That in turn has to be

validated by the chip, which then generates a transaction certificate cryptogram (TC) to complete the transaction. Although third parties are involved in the transmission of data, namely the ATM owner and the Link transmission system, the data is encrypted.

10. The card, on a magnetic strip, also contains identification and other data which enable the card to be used for non-chip transactions. The use of the magnetic strip is substantially less secure than the use of the chip technology. In February 2006 it was still possible for a card with a chip to be used in a non chip, or backup, transaction at an ATM, where the data on the magnetic strip was used to achieve the transaction. By later in that year a change was made that now results in transactions being declined if a chip card attempts at an ATM with a non chip transaction. However, I am satisfied on the evidence of Mr Brown that the transactions with which this case is concerned were transactions recorded by the system as having been processed by chip. He explained that had the backup strip information been used, and not the chip, the printout of the transaction would have had different features. Thus in this case we are dealing with transactions recorded by the system as having been carried out by the chip process briefly described above.

11. Mr Brown relies on the transaction log, as explained by him, to prove that these transactions took place. More detailed information containing authentication data, including the ARQC, was retained for 180 days but is not now available. The logs available show standard transaction processing. The process of validation, steps in which can be traced, either results in an approved transaction or it doesn't. The card unique key is not held anywhere on the system and HBOS does not have a method of generating it. Mr Brown has seen, but has not produced, a record from the LINK system showing that transmission of data for these transactions took place. The bank relies on the assertion that even now, in 2009, there is no evidence that fraudulent chip and PIN cards can be produced, and that a systems fault that allowed withdrawals without the appropriate chip or PIN, or which showed transactions which had not taken place, would have resulted in widespread problems. The absolute out come of a complex and encrypted process is relied upon.

12. It is convenient to deal with the Claimant's position by listing the ways in which Dr Murdoch contemplated the system could have reached the result of showing these transactions even though neither Mr Job nor anyone connected with him had used his card and PIN. It is agreed that the cloning of Mr Job's card through "an invasive physical attack" is unlikely. There is currently no evidence that criminals are able to clone chip cards. Apart from such cloning, Dr Murdoch's list in his report is:

    (i) An error being made during design or personalisation of a card which makes it possible to extract the card unique key.

    (ii) An error during the personalisation process which results in multiple copies of the same card being created.

    (iii) An error of the authorisation or reporting process which causes it to report that a transaction has been successfully chip verified, when it has not been.

    (iv) A compromise of the personalisation process which allows a malicious person to know the card unique key or create cards with the card unique key.

    (v) A compromise of the authorisation server which allows a malicious person to carry out a transaction, despite the chip verification having failed.

13. Dr Murdoch said that he had recently been contacted by someone who had been sent 2 cards in the post several days apart, and he had tested them and found them identical. Some details of that event, including the bank's ultimate response at the end of the story, remained obscure. There was no evidence of the extent to which other possibilities listed had come about. Mr Baker said that if the transaction was cryptographically authorised then either the genuine card was used, or a "high tech" attack had been used to defeat the security checks.

As to the latter, APACS are not aware of high tech attacks having taken place with ATM transactions like these. Mr Baker said in writing:

> To my knowledge there have been no incidents of physical, procedural, personnel or logical controls being breached on any bank system that would lead to the successful attack to compromise the cryptographic keys. If these controls were to have been breached then we would expect to see a large number of cards compromised rather than just Mr Job's. Since the beginning of the chip and PIN programme over 300 million chip and PIN cards have been issued securely and we have no evidence of such a breach.

Mr Baker repeated in evidence that he knew of no reported instances of chip and PIN breaches with ATM's. Such events would not be kept secret. APACS would have to divulge such developments.

14. Dr Murdoch accepted that, though there were no public statistics on how often incidents occur that allow transactions to be recorded that are not authorised by the correct chip and PIN, it seemed likely that such cases were a small proportion of card transactions overall, so that it would be quite unlikely that any individual cardholder, selected at random, would be in this situation. He said in writing:

> This fact is not relevant in the case at hand, since both sides agree that Mr Job is disputing a charge which bank records indicate being a chip transaction. What is at question is whether it is more likely that the card issued to Mr Job was used to carry out the disputed transaction, or whether the transaction was carried out by a criminal without the authorisation of Mr Job. This depends on the evidence of the disputed transaction, and the likelihood of different explanations for the evidence, not the fact that such situations occur rarely.

In his oral evidence Dr Murdoch seemed to attach importance to, or at least to identify this case as unusual because of, the fact that Mr Job has pressed the matter as far as litigation. It did seem to me that a comparison of the likelihood of Mr Job's card and PIN being used (on the one hand) and any of the other possible explanations put forward (on the other) was being avoided.

15. It seemed to me that at the centre of the debate was the question whether the bank had produced enough information to prove their case. Have they disclosed enough to enable the history of the transaction and its integrity to be demonstrated. The ARQC, if it had still been available, would have shown that a chip transaction had been attempted. The unique number for the card would enable one to know that the correct card had responded. As to the unique number, it was Mr Brown's evidence, supported by Mr Baker, that the number is nowhere stored. It could be generated by the development of particular software, but the system is such that it cannot be produced. It is identified for the purposes of an individual transaction by the use of master keys of the bank's system, but a record of it is not made. I did not understand HBOS to be different from other banks in this respect of the non availability of cryptographic keys. Absolute reliance is placed on the proposition that if a chip transaction takes place the right keys have been used in the exchange between the chip and the bank's system.

16. For the Claimant, Mr Mason submits that it is for the bank to prove how the transactions actually occurred, for example to produce the ARQC's and the PIN, sufficient for the court to draw its own conclusions. He submits that the logs produced are not sufficient. It may be treated as part of the business records of the bank, but the process by which the printout is arrived at is obscure. The ARQC's would show that these were chip transactions. Those, and other original transaction data, appear to have been destroyed under the bank's policy, though they were initially available. It is said that it is for the bank to show that the card did not have any flaws that would enable the key to be extracted from it; that a strong random number generator was used; that there were appropriate controls on key management; and that there were appropriate controls on the personalisation process. The only evidence is identified as being Mr Baker's assertion that there has never been a key compromise in the industry. The assertion is only a

statement of the bank's ignorance. Although card fraud generally is prevalent, the bank has produced no evidence of the nature and number of frauds that affect chip and PIN cards. The case being made by the Defendants that these transactions did not have the common indications of fraud does not carry weight unless the common indications are identified. Moreover, transactions involving withdrawal of the maximum amount allowed on a daily basis for a week are not typical of the way in which Mr Job runs his account.

17. For the Defendants Mr Kramer submits that use of Mr Job's card with the correct PIN is by far the most likely explanation for these events. After physical cloning of the card is ruled out, a system failure or a super hacker would involve a profound compromise of the bank's systems. Such an event would have come to light in other ways, and would not just reveal itself by a series of withdrawals from Mr Job's bank account. The examples that the Claimant has raised during the course of the case, such as "yes" card cloning were not apposite to online chip and PIN transactions, nor were the cases referred to, for instance the Citibank criminal case in the United States, where a widespread fraud was perpetrated by hacking into retailers' systems to obtain card numbers and account information. Here the use of the correct PIN, which cannot be found on the card itself, and is transmitted in encrypted form, is to be considered in addition to the integrity of the chip.[1] All the explanations put forward are highly unlikely, compared with the probability of Mr Job's card being used.

18. Mr Kramer also makes submissions about the surrounding and attending circumstances:

    (i) If this was a fraud, the criminals would not have chosen a basic Electron card account, which cannot go into overdraft.

    (ii) Having the use of the card, a fraudster would not have confined himself to ATM transactions with a maximum of £300 per day, and without knowing the probably modest amount in the account, rather than trying point of sale transactions.

    (iii) The last attempted use of the card was the day before the matter was reported to the bank, and there were no attempts to use it thereafter, so if this was a fraud the perpetrator coincidentally stopped before the bank was alerted.

    (iv) The 2 ATM's concerned were close to the Claimant's house and ones which he used regularly.

    (v) The Claimant is in fact careless with his cards. In the few years he had an account he seems to have lost 7 cards. In addition 2 cards were sent to him, including a credit card, that he says he did not receive.

    (vii) Mr Job had already in 2005 obtained a refund after reporting non receipt of a credit card and PIN.

    (viii) No withdrawals other than the disputed ones were made during the period in question.

19. Although the expression "test case" is not applied to this claim by either side, it has provoked wider interest. It is clear that there is an uneasy relationship between the financial institutions and those involved externally in the security world, including the academic world. I was shown a blog or part of a blog headed "Chip and PIN on trial" which was written by specific reference to this case, and to which several people had contributed. There is a hint of small men whose cases have merit against the juggernaut corporation which will admit no wrong. It is also said to be the experience of customers who complain of fraud or a failure of

[1] *Note from the editor: Professor Ross Anderson has indicated that this is not correct. The PIN is actually stored on the card in clear, and it is transmitted in clear from the terminal to the card in merchant terminal transactions. In ATM transactions, the traditional way of dealing with PINs has been to encrypt them at the ATM and send them to the issuing bank for verification. Both of these are vulnerable to interception. In the case of a merchant terminal, it is possible to obtain the card details and PIN directly. In the case of an ATM, the attacker can switch a negative authorisation into a positive one, because the authorisation responses are generally not encrypted. The learned judge requested both counsel in the case to comment on his judgment before it was made public, but because I do not have a sufficiently detailed knowledge of the technical issues, regrettably I failed to alert the learned judge to this point.*

technology that they inevitably face a denial of liability and are unsuccessful with the ombudsman, as Mr Job has been. I mention those matters merely to emphasise that this is certainly not a test case, and has no wider forensic importance. It happens to be a case where the complainant has pursued the claim to litigation and trial, but, unlike Dr Murdoch, I do not attach any measure of evidential significance to that.

20. I do not accept the Claimant's proposition that each step in the process has to be expressly demonstrated. I do think that the absence of a history of successful fraudulent attacks on online chip and PIN transactions, and the absence of any evidence of systems failure, as showing that these were transactions that can be taken at face value, (both of which are supported by the evidence of Mr Baker and Mr Brown), are important pieces of evidence from which it is open to the court to draw the inference that these were transactions that took place using Mr Job's card and his PIN. That is a conclusion that I do reach in this case. The surrounding circumstances are a significant help in that, in particular that the withdrawals are all recorded as made at ATM's which the Claimant himself used near his home; that they stopped without the card being captured or rejected before the matter was reported; and that the transactions in question were all cash withdrawals and on one single Electron account to the extent of just over £2,000. Those circumstances in particular seem to me to add weight to the bank's case that this record of transactions does not appear because of systems failure or because of fraud. As was accepted a finding such as I have made means that the Claimant is not successful in the case, because his case that he had the card at all times and had never compromised the PIN must be rejected. I do not find quite how these withdrawals came to be made, only that they were made by him, or by someone authorised by him, or by gross negligence in that he had enabled someone else to use the card and have the means of knowledge of the PIN.

21. Although I have found the evidence, including that of the surrounding circumstances, enables the bank to prove their case, I do repeat that the decision has no wider significance. It is a decision of one Judge in the county court on the evidence that he has heard and considered. I do add this warning, however: In other circumstances and without surrounding evidence another court might give weight to 2 matters in particular. Firstly, the bank had and retained more detailed information from which the course of the transactions could be traced, but destroyed it after 180 days (in this case even after a dispute had arisen). I do not expect that the argument that the bank should develop the means to produce the card unique key, and should also produce it, will ever gain much purchase, but in other cases the failure to preserve evidence in its complete initial form may be held against a bank. Secondly, I do accept the caution of Mr Mason, echoing Professor Tapper, against the assumption that a computer system is necessarily working properly. The absence of relevant operational problems at the material time, and statistical evidence more carefully marshalled and demonstrated than by the witnesses here, could be a helpful and in some cases a necessary component of a bank's case.

22. In this case, however, I find that the bank has proved its case about these transactions on the balance of probabilities, and the claim must be dismissed.

The Order:-

IT IS ORDERED BY CONSENT that

1. The Claimants' claim be dismissed and judgment be entered for the Defendant.

2. The Defendant's costs of this action be paid by the Claimant within 14 days of the date of this Judgment, as follows:

   2.1 Fast track trial costs of £485 plus £345 under

CPR Part 46; and

2.2 Pre-trial costs and post-trial costs summarily assessed at £15,000.[2]

© His Honour Judge Inglis, 2009[3]

Commentary

The case of Job v Halifax plc was an interesting and significant case in respect of ATM withdrawals and the effect of Chip and PIN (personal identification number) technology.

Although the judge expressly stated that the case is not to be considered as a precedent, the case was carefully argued before him with respected expert witnesses and the judge gave a thorough and considered judgement. Consequently the case suggests the approach that courts in England & Wales will take in similar cases – which again will be decided on the particular facts.

Alain Job sued Halifax Bank of Scotland (HBOS) in March 2007 over eight withdrawals made from his account in February 2006. Job maintained that he did not withdraw a cumulative £2,100. He also maintained he did not authorize anyone else to withdraw the money. Mr Job decided to initiate legal action after the Financial Ombudsman Service (FOS), which mediates disputes between banks and customers, sided with HBOS.

Alain Job was an asylum seeker from Cameroon. He entered the UK in 2000, and was given the right to stay but was not permitted to work. He coped financially through the help of friends, charities and family. But owing to the UK immigration policy, he led a fairly chaotic life and had to move from one home to another. Following the dispersal policy initiated by the Home Office, he was moved to Nottingham where he received some 350 hate mails that forced him to move back to Reading. His wife died in August 2008.

Mr Job was represented pro bono by Stephen Mason, a barrister who wrote and edited the well regarded practitioners book on digital evidence *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis, 2007).

Prior to the hearing of the case, the author had a meeting with Stephen in which the author set out some of the history of ATM litigation in the UK, and thereafter with his agreement prepared a 17 page Witness Statement and 36 page Exhibit for use in the case if certain matters were not admitted by HBOS (see below) and attended the trial in case the author was needed to be called to give evidence. As matters turned out, the points the author addressed were not in issue in this case, and consequently the author's witness statement and exhibit were not used by Mr Mason and did not form part of the material placed before the court. Stephen explained that had they been used, because the specific facts were finally not in issue in this case, he might have been liable for costs.

Alain Job was the first person to sue a UK bank over a phantom withdrawal since Chip and PIN has been deployed. The bank relied on the purported electronic signature of Mr Job, and it was argued by Mr Mason that the burden of proof was on the bank to prove that it acted in accordance with the mandate, in that:

a. Cash in respect of each of the transactions was physically withdrawn from the ATMs.

b. Mr Job's card was used in each transaction.

c. Mr Job or a person authorised by him concluded the transactions, or that his carelessness enabled an unauthorised person to do so. Even if the correct PIN was entered into the ATM, it does not follow that Mr Job or a person authorised by Mr Job entered the PIN. A perfect forgery is nonetheless a forgery. The bank requires a PIN to be used, even though the use of a PIN acts to prevent the bank distinguishing a forged signature from a perfect signature.

One material possibility, raised by Stephen Mason, was that his card had been cloned. HBOS maintained that it was his exact card that was used to perform the withdrawals and consequently that either Mr Job knowingly tried to defraud the bank, or was grossly negligent in handling his card and PIN.

[2] *The amount submitted by Halifax PLC at trial for costs up to but excluding trial exceeded £36,000.*

[3] *Whether a judicial judgment is the copyright of the Crown or the individual Judge in England & Wales is not clear. In responding to the Gowers Review of Intellectual Property (HMSO, November 2006), Philip Leith, Professor of Law at Queen's University of Belfast submitted a short paper Copyright in the Digital Age: court judgments, in which he briefly illustrated the position of copyright of judgments in Ireland and the UK (considered to be unsatisfactory), and suggested that both countries should harmonise the position in relation to the practice in the USA and the EU, available at http://www.hm-treasury.gov.uk/d/queens_university_of_belfast_237_kb.pdf. In the interests of clarity, Pario Communications Limited does not claim ownership of copyright in this judgment. His Honour Judge Inglis granted permission for the judgment to be published in the Review through Susannah Nightingale, District Judges Listing Officer at Nottingham County Court, in an exchange of e-mails with the editor on 1 June 2009.*

HBOS, though their counsel, suggested that Mr Job had been careless with his cards noting the fact that he had been through nine cards in six years and, having discovered the disputed transactions on his last card, had not reported the matter by telephone the same night but had waited until the following morning. Mr Job, in evidence, retorted that he thought the card fraud centre closed at 10.00 pm and did not realise that it was a twenty-four hour service. During the course of his evidence, Mr Job admitted in respect of previous ATM cards that he had twice claimed that he had never received the card or the PIN and that consequently HBOS had reimbursed him for withdrawals on these cards because the bank could not prove that Mr Job had received the cards and PIN. He also admitted, at one point during testimony, to putting his ATM card at night under a kettle barbecue griddle drum in his garden for some inexplicable reason. Although it was not commented on by anyone at the trial, the only inference that could reasonably be drawn from this action was that Mr Job was concerned that someone in his house knew his PIN and could therefore have been making unauthorised withdrawals on his account. He also said in evidence, that having discovered the disputed transactions on his last card (nearly £3,000) when checking his balance at a shopping centre, he had not mentioned this loss to his daughters who were with him at the time – wanting, allegedly, instead to check the facts before raising the matter. This evidence, coupled with the kettle barbecue griddle drum evidence, gave rise to an implication that Mr Job did not trust the people around him and believed that his PIN may have been known by others.

The judge concluded that Halifax had discharged its burden and proved that Mr Job's card was used in the ATMs. He did not reach any conclusion as to how the withdrawals were made, only that they were made by Mr Job, or by someone authorized by him, or by gross negligence. In addition, the judge rejected the argument put forward by Mr Mason that the bank should prove each step in the process (cash withdrawn from the ATM and evidence of the ARQC).

ATMs prior to Chip and PIN – the legal position before 2006

In 1992-3, the author was counsel in a Group Action against all the UK banks and building societies representing around 2,000 plaintiffs and potential plaintiffs. At that time, ATM cards had no security features such as Chip and PIN but were simply magnetic stripe cards. Indeed, one bank issued the same PIN to all its customers.[4] In May 1993 in a preliminary point of law, the author managed to get the banks to make the following formal admission: *A bank is not entitled to debit its customer's account unless it has the customer's mandate to do so*. The normal rules of evidence apply and the burden of proof is on the bank to prove that all withdrawals had been made in accordance with the customer's mandate.

A mere entry on a bank's computer system indicating that cash had been withdrawn by use of an ATM card and a PIN does not prove that a withdrawal had been made in accordance with the customer's mandate. There must be evidence showing that the customer in person entered the PIN. This remains the law. In April 2009 in the Job case, HBOS effectively admitted that the above position was still the law. However, today the technical issues that arise from Chip and PIN have complicated the matter.

The technical issues in Job v Halifax

As can be seen from the judgment, His Honour Judge Inglis accepted printouts from log files to show that Mr Job's card had been used for the transactions, even though the log files are secondary evidence and do not necessarily prove that Mr Job's card had not been cloned. The log files comprised of information that was sent by the ATM about a transaction to the bank's record system. Inexplicably, two primary pieces of evidence once held by Halifax were destroyed, including Mr Job's ATM card and the ARQC (Authorization Request Cryptogram), a piece of information generated from the encryption keys on the card that interacts with the bank's back-end systems. The ARQC would have shown whether the machine has read the card's chip. The lack of an ARQC record raised the possibility that it never existed in the first place, and that a cloned card was used or just a cloned card with a magnetic stripe. HBOS failed to present other primary evidence, namely the records from the ATM used in the transactions, and by the time that Stephen Mason became involved in the case, it was too late to require the production of this information by HBOS.

Of great interest was the fact that UK ATMs can be made to default to read the magnetic stripe if the chip is defective, thereby allowing a transaction to go through. Because HBOS was relying upon secondary evidence, it was not completely clear whether the ATM in question

[4] *Ross J Anderson, Security Engineering, (2nd edition, Wiley, 2008), 340.*

had defaulted in this manner – there was a clear lack of forensic computing evidence that could have established the fact conclusively. In the printout, the witness from HBOS asserted that the highlighted '04' bytes meant that the transaction had been validated against a Chip. But the defence experts who were not given access to the systems that generated the '04' bytes could not check this statement. Nor were the defence experts given anything other than a description of the validation system in the vaguest of terms.

None of the technical evidence presented suggested that criminals currently can clone a microchip for a Chip and PIN card, although security researchers have done this.

What was of specific interest is that it was admitted that Chip and PIN frauds are taking place because cards are being cloned without the chip and then used in countries where their ATM cards have not yet implemented the Chip and PIN technology. The judge mentioned in the course of the hearing that he too had had his ATM card cloned and used 'to buy pizzas in Essex', adding that he had not been to Essex in decades.

Conclusions

This judgement by a thoughtful judge bears careful scrutiny. A small ray of sunlight has been shone on the inner workings of banking security practices, and many lawyers now know what to look for. One important difficulty for anyone wishing to litigate against a UK bank has been the risk of the bank seeking costs against them – and pursuing the matter by asking for an order for attachment of earnings and charges on homes. Mr Alain Job was therefore, in some respects, the ideal claimant: someone who had no assets, lived in rented accommodation and by law was not allowed to take paid employment. In making his order, the judge ordered that Mr Job pay £15,000 towards HBOS costs, but this order will never be satisfied because there are no assets which could be attached.

A prudent banker should look at this judgement and make some changes to domestic banking procedures. All primary digital evidence, such as the ARCQ, needs to be systematically retained in archival form so that it could be produced if required. All ATMs should have their daily records archived for a similar reason. And there is no good reason why a pinhole digital camera should not be built into all ATMs with the photographs stored with the records – storage costs today are minimal, any data protection and privacy issue is false, because the photograph could only be used in preventing or prosecuting crime.

Following the case, Stephen Mason has put some very relevant and useful notes on his website (http://www.stephenmason.eu), setting out the issues and making practical suggestions on what to do if you believe that you have suffered an ATM fraud. In addition, the author has also prepared a 'Preservation Letter' that requires the bank to preserve all the evidence. The aim of this letter is to act as a mechanism to put the card issuer on notice of the dispute, and setting out what evidence should be retained by the card issuer. This letter is published below (and is available as a free download from the author's web site).

'Preservation Letter'

[your address]

[their address]

[date]

Request for preservation of evidence in respect of ATM transactions

Dear Sir or Madam,

ACCOUNT NUMBER: xxxxxxxxx

As you are aware I am currently in dispute with you in respect of certain ATM transactions on my account, which I write to confirm that I did not make or authorize. There transactions are:

[date] [Description from Bank Statement] [£Amount]
[date] [Description from Bank Statement] [£Amount]
[date] [Description from Bank Statement] [£Amount]

Under the law, when matters of this kind are in dispute,

the burden of proof is upon you to establish on a balance of probabilities that I have made or authorized the transactions listed above once I have told you that I have not made or authorized them. In this regard I respectfully direct you to Section 24 of the Bills of Exchange Act 1882.

My request

Accordingly, pursuant to the Civil Practice Rules and specifically the legal requirement that, upon notice being served upon a party in respect of a dispute, there is a duty to preserve all relevant evidence both in support of and against the dispute, I require you to preserve all relevant evidence in respect of your ATM system and the disputed ATM transactions listed above, pending the determination of our dispute.

This shall be done in the following manner:

1. In respect of the disputed ATM transactions, I require you to preserve the complete chain of transactional custody from the moment the alleged transaction was communicated to you. This shall include all transactional logs and error reports including any and all communications between your computers, computers belonging to or operated by corresponding banks (or other financial institutions), the ATM terminals alleged to have been used in the disputed transactions, the magnetic stripe on the ATM card and the Chip on the ATM card. Without prejudice to the forgoing, this data shall include all the ATM receipts and all the ARCQ (Authorization Request Cryptogram) information. It shall also include all metadata, error logs, system reports, engineers' reports, maintenance schedules, software and software updates in respect of the complete system so that it is possible to establish the precise state of each and every component involved in the disputed ATM transaction. If you have CCTV images or other independent evidence surrounding the disputed transactions (e.g. serial numbers of bank notes in the ATMs) this too shall be preserved. If you are aware of CCTV images or other independent evidence that may be retained by others in the vicinity of the disputed transactions, then you should seek to have this preserved as well.

2. In respect of all ATM transactions, I understand that you will have reports from internal audit and from security consultants on the security (or otherwise) of your ATM network and its vulnerability to fraud (both internal and external). While I am prepared to admit that these are confidential documents, they are not privileged documents and I require you to undertake to preserve them and in due course, if this matter proceeds to litigation (or adjudication by the FOS), to list each and everyone of them, together with the reports of actions taken to counter the vulnerabilities raised by these reports.

   [If the customer still has the card] I still have my ATM card, which I am keeping in a safe place. I understand that the ATM card is meant to contain within it what is termed an Application Transaction Counter (ATC). This ATC is incremented by one each time a transaction is initiated. Should you so wish, and at your expense, I am prepared to give my ATM card to an independent digital evidence specialist to enable him to establish whether the ATC has been incremented in accordance with each and every ATM transaction upon my bank statements or whether there are any discrepancies. To enable this to be done, you are to provide the independent digital evidence specialist with full cooperation in respect of his enquiries.

   [If the customer no longer has the card because he returned it to the bank] I returned my ATM card to you on [Date] and I trust that you have kept in securely. I understand that every ATM card is meant to contain within it what is termed an Application Transaction Counter (ATC). This ATC is incremented by one each time a transaction is initiated. Should you so wish, and at your expense, I am prepared to give my ATM card to an independent digital evidence specialist to enable him to establish whether the ATC has been incremented in accordance with each and every ATM transaction upon my bank statements or whether there are any discrepancies. To enable this to be done you are to provide the independent digital evidence specialist with full cooperation in respect of his enquiries.

Accordingly within 14 days of the date of this letter you may either:

1. Reimburse me with all the disputed ATM transactions listed at the start of this letter; or

2. Confirm that you have preserved all the above information pending the determination of this dispute. If you have been unable to preserve any of the above information, you must notify me of this fact in your reply.

Yours faithfully,

Alistair is a barrister with engineering and computing qualifications. Following 25 years at the intellectual property bar he moved into industry as a legal technology consultant and web developer. Today he works as a Digital Evidence Specialist Witness and as a consultant to high tech businesses and start-ups.

http://www.alikelman.com
ali.kelman@gmail.com