Chip & pin fallacies

Date: 16 October 2009
Authors: Stephen Mason & Roger Porkess
Issue: Vol 159, Issue 7389, New Law Journal

Recent cases have raised questions about the safety of chip and pin cards from fraudulent attack, for example by cloning. Typically, in such cases, the claimant is an individual whose account has been debited as a result of one or more allegedly unauthorised card transactions; the defendant is a bank or building society.

Recent cases have raised questions about the safety of chip and pin cards from fraudulent attack, for example by cloning.

Typically, in such cases, the claimant is an individual whose account has been debited as a result of one or more allegedly unauthorised card transactions; the defendant is a bank or building society.

A common counterclaim for damages for breach of contract is that the claimant did not observe the security conditions attached to the card and so made it possible for it to be used fraudulently.

In such cases, at least one disputed transaction has taken place. The question before a court is which of four possible explanations is the most likely, although they may not all be mutually exclusive:

A thief has stolen the money from the bank following a breach of the card's security.

A thief has stolen the money without a breach of the card's security.

The claimant is making a dishonest claim.

The bank has made an error.

This article is based on a survey to provide information about these explanations. Those taking part were A–Level mathematics teachers attending a conference in June 2009; 250 questionnaires were given out and 80 returned.

Only card transactions from January 2006 onwards were considered, post-dating the introduction of chip and pin technology. The survey was based around people's experience with their banks and building societies.

These institutions use software designed to detect suspicious transactions; when such a transaction is detected, they contact the card holder to check whether they should make the payment.

The findings

Forty-six respondents had been contacted by their banks, many of them several times. Most of the transactions had in fact been authorised, but 11 of the 46 people had been contacted about unauthorised transactions. Of the 11 with unauthorised transactions, three could explain them as security lapses (typically losing the card) but nine could not (one person was in both categories).

The survey then went on to ask about unauthorised withdrawals; these cases had not been detected by the banks' detection software. Twenty-one people had had unauthorised withdrawals. Of these nine people could explain them as security lapses and 13 could not (again one person was in both categories).

Comments

The data from the survey makes it possible to say something about the probabilities of three of the four explanations. The starting point must be that a disputed transaction has occurred. The question then needs to address the relative probabilities of the various possible explanations.

Miscarriages of justice have occurred because courts have equated the probability of someone being innocent with the probability that the event occurred in the first place, rather than with the probability of an innocent explanation given that it has occurred. (This error is known as the Prosecutor's Fallacy.) The first two explanations of what occurred presuppose the transaction was definitely a fraudulent attack.

The survey identified 42 such attacks. Thirteen of these attacks could be explained by security lapses and 29 could not. So the data would suggest relative probabilities of 13/42 and 29/42 for the two explanations. These are too close together to justify a balance of probabilities argument in favour of either explanation.

Many of those who did not return the questionnaire may have felt they had nothing interesting to report. That would not affect the figures of 13/42 and 29/42 which are derived from the 42 cases where something had gone wrong rather than the 80 people who returned the questionnaire. This is not, however, the case when it comes to considering the third possibility, that the claimant is deliberately trying to defraud the bank.

The total of 29 unexplained attacks were reported by 16 individuals from the 80 respondents. This would suggest a probability of one in five, that a randomly selected individual has experienced an attack.

There are two problems with this estimate. If all those who did not return the questionnaire had nothing to report, the probability would reduce to about one in 16. More importantly, the claimant is not a randomly selected individual but one of a very small group of people involved in such cases. However, the importance of this probability is not its actual value, but that it is not zero. Such attacks can happen, and so it is entirely possible that the claimant is telling the truth.

This is the extent of the interpretation that is possible from this figure. Whether the court judges the claimant to be telling the truth must depend on other evidence.

These figures are alarming. They show that the chip and pin technology and the associated systems are far from secure, assuming (realistically) that the responses are truthful.

It should be noted that all the probabilities in this article were estimated from a small non-random sample in a dynamic situation, in which banks and fraudsters try to outwit each other, and so their values should be treated with caution.

However, it should be noted that the magazine Which? conducted an online survey of 1,038 members of the public in May 2009, and the findings of this survey seem consistent with the survey

noted above, in that 14% had money taken from their bank account and 13% had money taken from their credit card.

Regardless of what assertions are made by the banks with respect to the security of their systems, the evidence suggests that their systems are not as secure as they maintain.

To test the fourth explanation, the claimant will need to obtain disclosure of a variety of documents including, but not limited to, the bank's systems and procedures.

The survey findings are at odds with the judgment in the case of Job v Halifax plc, given on 4 June 2009. Mr Job had a total of £2,100 withdrawn from his account in February 2006 in eight withdrawals. He said he had neither made them himself nor authorised any third party to make them.

In his judgment, Judge Inglis stated, at [20]: "…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…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."

The banks

The starting point for the survey was whether, and how often, people had been contacted by their banks about suspect transactions. Over half the respondents had been contacted; the total number of queries was 158. Of these, 16 were unauthorised and could not be explained by lapses of card security.

In those cases, the banks put a stop on any further withdrawals being made. The survey then asked about unauthorised withdrawals that had actually been made. There were 13 of these that could not be explained by security lapses.

These figures show that the banks take measures to detect unauthorised transactions, but that their processes are still not very effective. They suggest that only about half of unauthorised transactions are detected in advance; however, to achieve even that level of success, a large number of transactions are investigated, about 90% of which are authorised.

That the banks are prepared to bear the considerable costs that are involved in the process of carrying out checks in this manner could be taken as an indication that they recognise that a security problem exists.

The survey then invited respondents to say what happened when they discovered that unauthorised withdrawals had been made from their accounts.

Ten out of the 13 people involved provided information, and nine of them had had the money refunded by the bank. Below are the comments from two of the respondents:

"The bank described two transactions to me in the space of three or four hours. One for about £40 in a Marks and Spencers in London and the other for over £500 at an expensive restaurant/club in London. I was in Paris at the time of these transactions. The bank refunded both amounts after I filled in a form. They didn't require me to prove that I was not responsible for the transactions. I assume that someone had managed to clone my card somehow.

“I contacted the bank and they confirmed that the debit card had been used online to order goods from a large supermarket chain for delivery to an address that was not mine and in another part of the country. The amount was refunded within a fortnight, the card was cancelled and a replacement card issued.”

However, one person had not been refunded and another spoke about a friend in the same situation.

The Ombudsman

With one case of someone who had not had money refunded (and information about another) the survey was too small to provide information for a reliable estimate of how many people have these experiences in any year.

However, the next course of action for someone who fails to get money refunded is to contact the Financial Ombudsman. Each year the Financial Ombudsman produces an annual report in which figures are published on the complaints about cash machines.

For the year ending 31 March 2008, there were 883 complaints, as opposed to 291 for the year ending 31 March 2007. No indication is given as to how many of the complaints were upheld. However, with such large numbers, it is almost inevitable that some complaints are incorrectly rejected.

The survey data came from A–Level mathematics teachers. They are a highly coherent group of people, probably better able than most to present their case to a bank. There is a danger that some people do not get a refund from their banks because they do not express themselves well, and that the same could be true if they go to the Ombudsman.

Taking legal proceedings

The decision to initiate legal proceedings is fraught with anxiety: by the time legal action is contemplated, much of the evidence might have been destroyed by the card issuer; finding a lawyer who is familiar with digital evidence is exceedingly rare, even in the twenty-first century, and the most effective deterrent of all is the fear of being liable for the other party’s costs where a case is shifted out of the small claims track owing to the complexity, and thereby depriving the claimant of the shield against costs orders.

Stephen Mason is a barrister.
Website: www.stephenmason.eu;
http://www.stephenmason.eu/articles/banking-the-pin-and-the atm/
Roger Porkess is the chief executive of Mathematics in Education and Industry. Website: www.mei.org.uk
New Law Journal electronic edition.
Website: http://www.newlawjournal.co.uk/nlj/content/chip-pin-fallacies