

Ross Anderson FRS FREng
Professor of Security Engineering

Eve Russell
17 Pinewood Drive
Potters Bar
Herts EN6 2BD



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory

August 15, 2011

Dear Mrs Russell,

Your dispute with Barclaycard

Thank you for the copies of the documents in your dispute with Barclaycard.

I have had a research interest in disputes involving payment systems since I came to Cambridge in 1992; before then I worked in the industry from 1986–91 as a consultant on the engineering of such systems. The papers that colleagues and I have written on fraud against EMV systems and against the earlier magnetic strip systems can be found on my website, www.ross-anderson.com. I've consulted for banks, and for customers in dispute with banks; I have acted for both the police/CPS and the defence in criminal matters; I have been called to testify before various parliamentary committees here and paid to write reports for both the European Commission and the US Federal Reserve.

It is clear that no proper investigation has been done in your case; the bank does not even know where their courier delivered the card and has not provided the logs that would let you discover when the alleged transactions took place.

It is quite wrong for the adjudicator (or the bank) to expect you to explain what happened. Under the Payment Services Regulations 2009 section 60 it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency. Barclaycard has failed despite repeated demand to do this.

The adjudicator is also mistaken in claiming that the only possible explanations are card cloning, card theft and fraud by yourself. In fact, this case fits the classic pattern of fraud by an insider.

Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD
England

Tel: +44 1223 334733
Fax: +44 1223 334678
E-mail: Ross.Anderson@cl.cam.ac.uk

Bank insiders frequently discover flaws in internal control procedures that enable them to issue cards and PINs on customer accounts. An early documented case was R v Moon at Hastings Crown Court in February 1992, reported in the paper 'Why Cryptosystems Fail' which you can download from my website:

... a housewife from Hastings, England, had money stolen from her account by a bank clerk who issued an extra card for it. The bank's systems not only failed to prevent this, but also had the feature that whenever a cardholder got a statement from an ATM, the items on it would not subsequently appear on the full statements sent to the account address. This enabled the clerk to see to it that she did not get any statement showing the thefts he had made from her account.

This was one of the reasons he managed to make 43 withdrawals of £200 each; the other was that when she did at last complain, she was not believed. In fact she was subjected to harrassment by the bank, and the thief was only discovered because he suffered an attack of conscience and owned up.

If memory serves, the housewife in question came to Ian Moon's attention because she had a credit balance of £12,000 in a current account for which she received annual statements. This signalled to him that she was not paying much attention to that account, so he would have some time to loot it before she noticed. I have come across a number of such cases since.

Your case fits this pattern. First, you had a high credit limit of £10,000, with very few transactions on the account; second, you were not paying attention to it by checking it regularly online.

The next point concerns the profile of victims. Over the past twenty years – since I switched from being an industry insider to being an outside expert – a steady stream of victims such as you have come to me after suffering card fraud and being wrongly accused by their banks of complicity. There are very few middle-class white men among their number. Those victims of disputed transactions who are refused compensation by the banks and by the Financial Ombudsman Service (as well as by its predecessor the Banking Ombudsman) tend to be disproportionately female, ethnic minority and/or elderly. The reason for this, I believe, is that the first responders don't have access to logs or the resources to do proper investigations; as you can see from the correspondence they are barely even literate. They have to take a view based on limited information which includes whether the customer account is profitable and may include an assessment of whether they reckon he or she could put up a fight. In such a decision, psychological heuristics and biases, including cultural stereotypes, are likely to play a role unless positive measures are taken to neutralise their effect.

We raised the issue of racial and gender discrimination with the Financial Ombudsman Service in the submission I wrote with Nicholas Bohm on behalf of the Foundation for Information Policy Research (www.fipr.org) to the Hunt Review of the Financial Ombudsman Service (see section 19 of our submission, which you can get from FIPR's website or from mine). I am surprised that, three years after formally being put on notice that they may be engaged in or complicit in unlawful racial and gender discrimination, the Financial Ombudsman Service seems to have done nothing about it.

Furthermore, following the Reddell case described in Appendix B of our Hunt Review submission, I visited Dame Sandra Dawson, the Master of Sidney Sussex College, who is a non-executive director of Barclays Bank. She was shocked to learn of the pattern of racial and gender discrimination and told me that as Barclays did not monitor such things she did not know how the bank could defend itself against such allegations as it did not keep the relevant records. No doubt by now they have robust monitoring systems in place, and should they proceed against you further in the event that the Ombudsman does not uphold your appeal, you will no doubt be able to demand the figures. However an entrenched culture of discrimination against outsiders and the less well off may take some time to dispel and I note you report that the first two staff you dealt with were personally hostile. An insider selecting victims for fraud would be well aware of the internal culture.

The third way in which these transactions fit the pattern of an insider job is that the disputed transactions took place in central London rather than near where you live. Twenty-five years ago, insider frauds were often local to the victim because the crooked insiders were typically branch staff: the fraudulent transactions made by Ian Moon were at ATMs in Hastings. (In fact, at the time I worked in the industry it was common for a bank to sack 1% of its staff every year for fraud and embezzlement.) Things have changed somewhat since then as many branch staff have been replaced by people in call centres and other central locations. I first came across a centralised insider fraud in 1992 when London-based IT staff of a clearing bank used their systems to work out the PINs for stolen cards (this case is also noted in ‘Why Cryptosystems Fail’).

Finally, insider frauds often leave some suspicious telltale because of the procedural vulnerabilities that insiders typically exploit. In your case I note that there was a link in your credit reference agency file to Brindley House, Alfred Road, London W2, which appears on Google Streetview to be a building covered with scaffolding and under renovation. Sending stolen goods – or a replacement card and PIN – to a building site is an old trick; combined with the fact that Barclays could not explain who their courier was or where he delivered the card, and the fact that they cannot find the voice recording of the call that was allegedly made to order the new card, this just cries out for explanation.

To sum up, Barclays have failed to keep proper records and have failed to investigate this case properly. This is also part of an unfortunate pattern. In my experience banks are ever more reluctant to prosecute or even investigate insider fraud; the reputational risk and internal bureaucratic complexity can appear daunting and other explanations are usually sought first. In the Reddells’ case, for example, it seems that their card was cloned after being used in a Barclays ATM in Peterborough, along with many other cards; this will surely have been known to the branch staff and the ATM team but the fraud team at Barclaycard were clearly unaware of it and sent the debt collectors after the Reddells. It may well be that in your case too the explanation is a corrupt insider elsewhere in the bank who might even have already been detected and sacked – while Barclaycard being unaware of this recklessly continues to harrass you for payment. If this is in fact the case here then the bank is committing an offence under Section 2 of the Fraud Act and its directors are personally committing an offence under section 12.

Should the bank proceed against you in court to try to recover the disputed amount I would suggest that you demand discovery of the relevant logs, records, procedures and statistics of internal investigations including ethnic and gender compliance monitoring.

You also asked whether bank insiders have access to customer PINs. You note that this is an issue on which the bank appears to be evasive. The answer is yes.

PINs for both mag-stripe and EMV (‘chip and PIN’) transactions are, by industry standards, managed using devices called hardware security modules or HSMs. A bank the size of Barclays might have about 300 of them scattered round various data centres. The concept is that the PINs are generated and verified in the HSMs using keys kept there; HSMs also manage keys used to encrypt PINs in ATMs and the keys loaded into bank cards. In theory, no member of bank staff should ever get hold of a PIN other than his own. Practice is very different from theory, and we documented extensively in a series of papers how API attacks can be used to extract PINs and keys from HSMs. The technology dates back to the 1980s and is no longer really fit for purpose. In addition to direct technical attacks, I have worked on cases where insiders got access to PINs either by abusing the authorised mechanisms provided for PIN issue or reissue, or exploiting system misconfigurations and failures. There have also been cases where insiders colluded with outsiders (so Barclays’ failure to name their courier company arouses extra suspicion).

I note that in Barclays’ final letter to the Ombudsman of December 30th, Judith Hayes writes ‘our investigations have led us to conclude that we cannot be certain the spending was not carried out by Mrs Russell or with her knowledge’. In effect she is insinuating that you colluded in the fraud and inviting the ombudsman to place on you a burden to disprove this, not just on the balance of probabilities but beyond reasonable doubt. This is not just in blatant disregard of the Payment Services Regulations 2009 but speaks volumes about the banks’ expectations of the ombudsman, on which we elaborated in our response to the Hunt Review. The banks seem to have come to expect that if they say ‘chip read, PIN used’ the ombudsman will say ‘bank wins’ regardless of the law or the facts.

I will copy this letter to Dame Sandra with the suggestion that she have your case looked at by someone in the bank with clue. I am happy for you to copy it to the ombudsman; you might perhaps ask for your appeal to be held by the Chief Ombudsman and let her know that you'll publish the case papers afterwards regardless of the outcome.

If the ombudsman's final decision in your case continues the sad pattern of the Reddell and Truong cases and flies in the face of both the law and the facts, then I would suggest you make a formal complaint to the European Commission – that the UK is failing to discharge its obligation under section 51 of the Payment Services Directive to 'ensure that adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and their payment service providers are put in place for disputes concerning rights and obligations arising under this Directive, using existing bodies where appropriate.' You might also send copies of the papers to Suma Chakrabarti at the Ministry of Justice as the accounting officer responsible for the Financial Ombudsman Service.

Yours sincerely,

A handwritten signature in blue ink, appearing to read 'Ross Anderson', with a horizontal line underneath.

Ross Anderson