Ross Anderson FRS FREng
Professor of Security Engineering

Melanie Johnson
UK Cards Association
2 Thomas Moore Square
London E1W 1YN

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

December 2, 2011

Dear Ms Johnson,

Responsible disclosure and academic freedom

Your letter of April 4th to Graham Allen has been passed to me for information. You try to redefine 'responsible disclosure' to mean that the researcher should only inform the vendor or operator of a security vulnerability, but never disclose details publicly, contrary to settled industry practice. You also try to associate public disclosure with the provisions of section 44 of the Serious Crime Act 2007 (intentionally encouraging or assisting an offence) despite the fact that there is no intent on the part of security researchers to encourage or assist offenders.

The University's response to you dealt adequately with your substantive complaints and I will say no more about them. However, since you raised the possibility of criminal offences relating to bank fraud, I would like to draw your attention to Section 2 and Section 12 of the Fraud Act 2006. You are in breach of Section 2 if you dishonestly make a false representation, and intend by making the representation to make a gain for yourself or another, or to cause loss to another or to expose another to a risk of loss. A representation is false if it is untrue or misleading, and you know that it is, or might be, untrue or misleading. Under Section 12, if the offence is committed with the consent or connivance of a director, manager, secretary or other similar officer of a body corporate, they (as well as the body) are guilty of the offence and liable to be proceeded against and punished accordingly.

I refer of course to the frequent statements made by UKCA and by its predecessor APACS to the effect that the UK banks' card payment systems are secure, when in fact they are not.

Cardholders in Britain experience payment card fraud and forgery running into hundreds of millions a year. Cardholders suffer debits they do not recognise; but when they complain they are often told by their bank that as the system is secure they must be mistaken or lying. Up till 1992, the banks themselves made the public claims of system security; since then APACS has taken over that role, followed by UKCA. We have recorded many examples.

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

- Since the introduction of EMV ('chip and PIN') in 2005 your spokesmen have repeatedly claimed that no UK ATM would perform a mag-strip fallback transaction for a UK-issued chip-and-pin card. We tested your assertion in 2006, 2007 and 2008; it turned out to be false.

- Your website described a number of PIN Entry Devices as 'Common Criteria Evaluated' against a protection profile which claimed that compromising any instance of them should cost at least $25,000. After we demonstrated, on Newsnight in 2008, that the widely-used Dione and Ingenico devices could be trivially compromised, you claimed that they had not actually been certified according to the Common Criteria, but rather using a similar methodology of your own about which you were not prepared to disclose further details. The Common Criteria claim was therefore misleading. Your spokesman then claimed that criminals would not be sufficiently skilled to mount such an attack, and this claim was false as they already were doing just that. PIN entry devices were being compromised as they were shipped through Dubai, and although the perpetrators were arrested the prosecution collapsed – apparently because you and your member banks were not prepared to cooperate.

- Your spokesmen have at all material times denied that chip cards can be cloned, despite regular reports of yes cards being used in other European countries. If you are ignorant of yes cards and SDA fallback attacks, you are incompetent, while if you deny their existence despite knowing of them, you're probably committing Section 2 offences.

- As a specific and serious example of your policy of denying well-known vulnerabilities, your David Baker signed a witness statement in the case of Job v Halifax in 2009 (reported in volume 6 of the Digital Evidence and Electronic Signature Law Review) in which he testified to the truth of what he had stated, and claimed that magstripe fallback was not available in any UK ATM for cards issued in the UK. When placed on the witness stand, and on oath, he then reversed this comment.

The effects of this wilful and systematic misrepresentation on customers have been severe. The Financial Ombudsman Service, which you constituted in its present form via the Financial Services and Markets Act 2000 which you personally steered through Parliament, routinely relies on the security claims falsely made by the UK Cards Association which you now chair in order to decide disputes unfairly in favour of banks and against their customers. I draw to your attention the case of Donald and Hazel Reddell whose Barclaycard was cloned after they used it in a Barclays ATM in Peterborough, at a time when many other cardholders in that town reported phantom withdrawals. The ombudsman relied on your untrue claim that fallback mag-strip forgery was not possible and found against the Reddells, a vulnerable elderly couple who did not have the resources to fight Barclays in court. They were intimidated into paying some £3000 by debt collectors sent by the bank even while their case was before the Ombudsman. Their case documents are online and in view of the assurances in respect of the European Convention on Human Rights that you gave to the House of Commons in November 1999 when you took the bill through its committee stage, I suggest you read them carefully:

`http://www.fipr.org/080116huntreview.pdf`

That case is just one of many. It should shame you as a former member of a Labour Government that the fraud victims who come to us having been brushed off by their banks and by the ombudsman are disproportionately the more vulnerable members of society – minorities, female and the elderly.

It may have seemed like a good idea in the 1990s for APACS to make security claims on behalf of banks so that a banker could not so easily be accused of fraud if he made a false security claim about his own systems. But the Fraud Act 2006 clarified matters, having been framed inter alia to bring ATMs and chip-and-pin readers properly within the remit of fraud law. Since it came into force on January 15th 2007, whenever a body like UKCA makes a false security claim about banks' systems to make a gain for its member banks, or to expose bank customers to a risk of loss, it commits an offence.

I now turn to the issue of mens rea, or intent, where your suggestion of criminal behaviour on our part falls down. Your case is different. There have been repeated TV and radio programmes on ATM phantom withdrawals and card fraud generally in recent years, exposing the untruths told about system security

by spokesmen from your organisation and its predecessor. The Reddell case, for example, was featured on 'Tonight with Trevor MacDonald', and as you know both the PED compromise and the No-PIN attack were featured on Newsnight in 2008 and 2010 respectively. Thereby UKCA's spokesmen have been repeatedly placed on notice that their security claims were false, raising a clear issue of offences committed by them under Section 2 of the Fraud Act. You cannot maintain that the false security claims are simply an honest mistake arising from your staff's lack of technical knowledge; Baker, for example, claimed to be an expert in court. It is quite evident that the false security claims were part of a policy of deliberate advocacy. The high levels of publicity surrounding these cases, and the annoyance caused to your member banks by your mishandling of them, ensure that UKCA directors have been more than adequately put on notice. By permitting the denial to continue, you were connniving at the Section 2 offences thereby committed. You and your fellow directors will therefore bear criminal responsibility under Section 12 if a jury is convinced that you acted dishonestly.

The *Ghosh* test is that your conduct will be held to be dishonest if an ordinary person would think it so. Even if your fellow directors of UKCA feel it proper "to defend the honour of the banks' systems", or however you might phrase it at your board meetings, it is still dishonest in law if it is seen as such 'according to the ordinary standards of reasonable and honest people'. The man on the Clapham omnibus does indeed consider it dishonest for banks to lie about the security of their systems in order to dump the liability for fraud on to cardholders and merchants; the many calls and emails from the public received by me, and by the producers of TV programmes on such cases, leave no doubt about that.

That is not all. You claimed in your letter of December 2010 that the No-PIN vulnerability no longer worked. It is indeed true that Barclays had their vendor consult us and implemented a partial fix; but when we performed some tests after I last wrote to you we discovered that the vulnerability was once more effective even when using a Barclays card in a Barclays terminal. Last month the BBC came round again and once more filmed a card being used without knowledge of the PIN in such circumstances. Yet in recent dealings with fraud victims, the Financial Ombudsman Service has once more followed your lead and maintained that a 'chip read' transaction with a PIN used was incontrovertible proof that the cardholder was negligent or lying.

You thus made a false representation whose intended effect was to make a gain for your member banks or to expose their cardholders to a risk of loss. By writing to the University of Cambridge with a view to suppressing public knowledge of the No-PIN vulnerability, which was still exploitable despite your false written assurance, you personally committed an offence under section 2 provided the Ghosh test is met. The public outcry that followed your letter should leave little doubt about that test in this case.

You are also, I believe, in breach of Section 44 of the Serious Crime Act 2007 by encouraging or assisting the commission of offences, namely the Section 2 Fraud Act offences by your member banks, and perhaps the activities of Mr Baker. 'Encouraging or assisting' is the very matter with which you tried to smear our team. But perhaps in your case a prosecutor would have no need to rely on charges involving incitement or conspiracy as the evidence of substantial direct offences committed both by the UKCA and by you personally is clear.

You might be tempted to take the view that as the chair of UKCA you are 'not available for arrest' any more than Mr Rupert Murdoch; indeed, the UK seems to have not sent any bankers to prison against the wishes of their employers since the 1930s. You no doubt have excellent relationships with law enforcment, given that you finance the police's Dedicated Cheque and Plastic Crime Unit and host it on your premises. But you might ponder whether you are more exposed thanks to the events of 2008 to which a major contributory factor was the damage that you yourself wrought while a minister to financial regulation in Britain by means of your Financial Services and Markets Act. If Britain ends up in economic circumstances similar to those of the 1930s, then perhaps bankers will once more go to prison. As a former Labour MP, you might even consider it a good thing, at least philosophically, that the police may be getting less reluctant to investigate the crimes of the rich and powerful; the sacking of the previous Commissioner of the Met may serve *pour encourager les autres*. You will just have to take advice, consult your directors and members, and take a view on whether you think it prudent to continue making false representations and conniving at your staff doing do.

For my part I believe that the UK Cards Association owes us a clarification and an apology, plus an undertaking to cease and desist from harrassing security researchers. The industry also owes victims such as Donald and Hazel Reddell not just an apology but a refund and compensation for the distress inflicted on them.

In the meantime, we will no longer make responsible disclosure of ATM, EMV and other financial system vulnerabilities to the UKCA but to the European Central Bank, to effective national regulators such as the US Federal Reserve and the Banque de France, and to individuals within the banking system with whom we have working relationships.

Finally, I observed your false representations being repeated this morning on BBC1's "Rip-off Britain". Although the producers of that programme exposed them adequately, you may be assured that any future repetition of the offences will result in an immediate and public complaint to the police, and especially where you attempt thereby to interfere with academic freedom.

Yours sincerely,

Ross Anderson