Failures on fraud

Online payment abuse is falling through regulatory cracks, writes **Ross Anderson**

This past year has been a challenging one for central bankers and regulators. Each economic downturn exposes problems built up during the exuberance of the previous boom, and recent problems – such as those of Fannie Mae and Freddie Mac in the US, and Northern Rock in Britain – have exposed some serious weaknesses in oversight.

We are now beginning to see systemic problems with payment systems that were built in a rush during the dotcom boom. Fraud against home banking systems, for example, is rising sharply. Phishing is the most rapidly growing new crime ever, having gone from nothing to a multibillion business in four years. The move in Europe to EMV (the standard for interoperation) payment cards has not led to the predicted fall in losses: while some types of fraud are down, others have grown rapidly. It's as if a bulldozer had been driven across the fraud landscape, diverting flows of wickedness but not damming them.

Lessons from PIN factories

However the problems in payment systems are being exposed not so much by the economic downturn as by the fact that since about 2004 fraudsters have started to specialise. Until then, fraud tended to be what can be thought of as a vertically integrated cottage industry: a gang would write wicked code, steal card data, make cards, buy goods and sell them. This placed limits on both sophistication and scale.

Now, however, criminal markets link malware writers, botnet herders, spammers and phishermen with money launderers and cash-out specialists. Adam Smith famously described how specialisation boosted the productivity of a pin factory in 18th-century Scotland and exactly the same process has industrialised the business of getting customer cards and PINs. Now, whenever a vulnerability can be exploited, it will be. Engineers in Russia or elsewhere will build machines to skim ATM cards, or software to run middleman attacks on bank websites, or whatever else they can. Criminal methods are developed quickly and they scale rapidly.

Passing the buck

The industry's reaction to technological threats is unfortunately no longer really fit for purpose. A recent example comes from EMV deployment. The use of PIN Entry Devices (PED) in millions of European retail outlets created a risk that they would be tampered with so as to collect card and PIN data for use in mag-stripe clones, and, indeed, this has happened since at least 2006. In 2007 two colleagues and I examined the most popular makes of PED in the UK and found that they were trivially easy to tamper.

Yet one of them had been certified as secure by VISA, and the other was said to have been evaluated under the Common Criteria, an international standard for computer security. We shared our results in October 2007 with APACS (the UK payments association), VISA, GCHQ (a British intelligence agency) and other interested parties. It turned out that the Common Criteria evaluation claim was a bluff: the device had not in fact been certified under the Common Criteria but merely "evaluated" using a process vaguely modelled on the criteria. When we finally published our results in February 2008, APACS argued that they were of no significance as actually attacking these terminals would be too hard. But at the time of writing, in August 2008, the police have just advised merchants to be vigilant against PED tampering, and a number of PEDs are being withdrawn from service.

Ross Anderson

Ross Anderson is professor of security engineering at Cambridge University. He is a founder of a vigorously growing new discipline: security economics. Many security failures are caused by wrong incentives rather than technical failures, and microeconomic analysis has shed light on problems once considered intractable. He has also made many technical contributions, having been a pioneer of peer-to-peer systems and hardware tamper-resistance. He wrote the definitive book: *Security Engineering – A Guide to Building Dependable Distributed Systems.*

It is perfectly understandable why both banks and vendors cut corners if they can: the costs of a compromise are widely spread. A bank that supplies its merchants with a cheap but easily-compromised PED saves millions at once, while the cards compromised later will have been issued by many different institutions. The negligent bank does not face the full economic costs of its actions, and the lucky vendors had their product "evaluated" by banking organisations with little incentive to look hard for problems. The stakeholders wanted to believe the assurances they got from other stakeholders, and no one had an incentive to blow the whistle (except academics, who can be ignored for a while). Thus the level of investment in system security was much less than optimal.

Customer beware

A second serious source of concern is the externalisation of risk to merchants and customers. Changing the liability landscape has been one of the goals of the EMV project: the holy grail was to blame the customer for a disputed transaction if a PIN is used, and the merchant otherwise. Yet this creates severe moral hazard. If the institutions that maintain payment systems no longer suffer the costs of failure, they will not work hard to keep these systems secure. There are ever more cases of distraught cardholders who have suffered fraud but who can get no redress.

In the UK, the House of Lords Science and Technology Committee has recommended changes in the law. Bankers are resisting this, but in my view this is myopic. Since the industrial revolution, the banking industry has reaped huge profits from trust service provision. In the 18th century, the London merchant banks had come to prominence by accepting merchants' bills, while in the 19th century the steamship and railway, supported by letters of credit and telegraphic transfers, drove a huge expansion of trade and bankers' profits. In each case, the effect was to enable merchants who didn't completely trust each other – and who perhaps had never met – to do business. This trust service has been hugely profitable for the banking industry. And it still is. Nowadays most internet transactions involve credit cards, so banks get a few per cent of the turnover via merchant discounts and fees. As in previous centuries, the business depends on consistently trustworthy behaviour by insiders.

Unfortunately, technology is increasing the temptation for institutions to free-ride, while simultaneously making enforcement more difficult. In the PED case, the FSA was not interested in technology, and the one UK government body with infosec competence – GCHQ – did not feel the need to defend its Common Criteria brand against passing off.

A new regulator

What is to be done? Colleagues and I studied information security economics and the single market in a project for the European Commission.[1] Our report makes a number of recommendations. The two of these that most directly affect the banking industry are that Europe should publish robust per-country statistics on electronic crime, like those already produced in Britain by APACS and in France by OSCP, and that we need European action to harmonise procedures for the resolution of disputes between customers and payment service providers.

The final question is where the regulation of payment services should be undertaken. The PED case shows that the answer is not just "VISA". Will it be "the central bank"? Alan Greenspan argues that central bankers should no longer decide whether a troubled bank should be rescued; there should be a separate body for bank rescues. Central bankers are too close to the banks they regulate and take too little account of the rest of us, whether taxpayers or customers. The ongoing failure of central bankers to take any real interest in either the industrial or consumer aspects of online fraud raises similar issues.

If central bankers don't care about the dependability of the payments system – let alone about the interests of bank customers and taxpayers – governments will eventually have to set up a new separate body to regulate payments. And if the police cooperation needed to fight globalised online crime is going to emerge at the European level, as our report recommends, then payment services should logically be regulated by Europe too. □

1. *Security Economics and the Internal* Market by Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore available at www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.