The Foundation for Information Policy Research

Consultation response on

The National Payments Plan

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

Background

Technology has made payments easier and cheaper. But recent developments have undermined the protection that bank customers enjoy against fraud and error, and there are growing problems with payment system security and resilience. These are linked. When payment service providers are able to externalise fraud risks by transferring them to customers, the incentives to protect systems properly are undermined. Further complications include the breakdown of the system of evaluation and accreditation of security systems. The problems extend from card payments to online financial services, and affect not just retail customers but also SMEs.

This is an example of regulatory failure. Payment service providers act in what they perceive to be their own best interests by minimising liability for transaction disputes, However the global result is far from socially optimal. Card fraud is rising; customer complaints are rising; consumer confidence is being eroded; and ultimately the UK will become a less attractive place to do business.

We are concerned that the National Payments Plan, as outlined in the consultation document, will make matters worse.

History

The common-law approach to forged payment instruments was codified in the Bills of Exchange Act 1882, section 24, according to which a forged signature was completely null and void. Accordingly the forgery risk was borne by the relying party, and a British bank could not use its terms and conditions to make customers liable for forged cheques (unlike, for example, in Switzerland). A bank wishing to debit a customer account had to show that it was acting in accordance with the customer's mandate.

Although the legal position has not changed, the practical protection enjoyed by customers has been eroded by a number of factors.

First, the UK suffered a wave of phantom withdrawals from ATMs in 1992–4 that led to the group action *McConville and others* v *Barclays and others*. In that case the judge

decided for the defendants who argued that the case should be broken up into numerous separate small claims, as there were no common facts. But the judge was mistaken. Many of the frauds had in fact been committed by one Andrew Stone and his associates. Although Stone was later imprisoned, the fraud victims for the most part did not get their money back. This fixed the UK banking industry in a pattern of behaviour whereby people who dispute transactions are told that since the bank's systems are secure, they must themselves have been responsible. Some egregious examples of this behaviour are documented in the FIPR submission to the Hunt Review of the Financial Ombudsman Service [1].

Second, the rush to online banking during the dotcom boom in the 1990s saw many financial service providers adopting terms and conditions that made a customer who accepted a password for online banking (or even phone banking) liable for any transactions that it was used to authenticate. See [2] for a survey of this.

Third, the growth of phishing and of keyloggers mean a significant and rising level of customer account takeover. With phishing in particular, it is not reasonably practical for the average bank customer to tell the difference between a genuine bank website and a fake one. For example, one of the big UK banks sent out a spam linking to a URL with an odd domain name. A recipient contacted the bank's security department, which told her it was a phish. Her son then contacted the ISP to report abuse, and found that the URL and the service were genuine – although provided to the bank by a third party [3]. When even a bank's security department can't tell spam from phish, how are their customers supposed to?

Fourth, the schemes for certification of payment terminals and other equipment don't work. PIN entry devices (PEDs) are certified both under a VISA scheme and under the Common Criteria; yet certified devices examined by independent experts turned out to be easy to compromise, and none of the stakeholders (APACS, CESG, or VISA) appears willing to take any remedial action – whether by decertifying insecure devices, changing the protection profiles and test criteria by which the evaluations are conducted, or decertifying the laboratories that wrongly certified devices as secure [4].

Fifth, the introduction of 'Verified by VISA' extends the process of risk dumping to online shopping. Until recently, payment service providers have borne much of the transaction risks of Internet business, and the industry has been richly rewarded by the growth of card turnover with income coming directly from merchant discounts and indirectly from the increased uptake of credit. But customers who accept the terms and conditions offered will find that much of the transaction risk is passed back to them (with much of the rest going to the merchants).

Sixth, there are substantial equality-of-arms issues in transaction disputes. The Ombudsman traditionally sides with the bank against the customer (see [1]); a bank can get CCTV images to prove that a customer made a disputed transaction, while she cannot usually get images to prove she didn't; and the UK costs rules make it infeasible for persons of normal means to sue banks, except in the small claims track (to which the

allocation of cases isn't automatic even when they fall within the relevant financial limit, and where the customer is still exposed to the risk of having to pay the expenses of expert witnesses).

Finally, the move to CAP authorisation of online banking transactions, whereby customers use their chip and PIN cards to compute authentication codes, will result in customers bearing more of the liability for online banking disputes – even although the quality of implementation varies very widely and it is quite predictable that the phishermen will use real-time man-in-the-middle attacks.

The upshot of all this is that a customer using old-fashioned payment mechanisms based on manuscript signatures enjoys a fair level of protection against fraud: a bank cannot debit her account without her mandate, and signatures on cheques are rarely forged so well as to seem genuine under forensic examination. But a customer using modern mechanisms based on online passwords or cards with PINs is much more vulnerable. Her PIN can be captured along with her card details by means of a wiretap in a merchant terminal; when she complains she'll be told it's her fault as the system is secure. She comes under constant pressure to acquire passwords for electronic banking; if she does so she's exposed not just to phishing risks via bogus websites but through the 'verified by VISA' mechanisms as well.

Thus a risk-averse bank customer might prefer not to have a password at all, and rely exclusively on cheques; and a normal but prudent and well-informed customer might use an electronic banking service for convenience, but keep the bulk of her savings with institutions from which she refuses to accept a password or a chip and PIN card.

Given this, no organisation mindful of consumer rights could support the proposed termination of cheque clearing.

Economics

Security economics can explain much of what is going wrong with the direction of the UK payments industry. Quite simply, financial institutions optimise their own short-term utility, but because of externalities, symmetric information and moral hazard, the resulting equilibrium is far from the social optimum [5].

For example, it might seem that UK banks are in a good position by virtue of having managed to externalise some of the fraud risk on the customer. However, the first ATM test case in the USA (*Judd* v *Citibank*) was won by the customer. Coupled with regulation E whereby in disputed transaction cases the customer's liability for unauthorised transactions is tightly limited, the opportunity for banks to transfer risks to their customers is very restricted. This has been documented in [6], and it turns out that the US regulatory regime is better: even from the banks' perspective, the total costs of fraud and security are less in the long run. One reason is moral hazard: UK bank staff are aware that customer complaints are less likely to be investigated properly (or at all) so they are less diligent when developing systems than their US counterparts [7]. Another may be due diligence: UK banks want to tick all the boxes so they can claim 'our systems

are secure', which makes it difficult to treat security and fraud as economic substitutes; meanwhile as US banks are exposed to the total costs of both fraud and security, they can take more rational decisions to trade off one against the other.

Phishing provides another example. In 2006, £34m of the UK's total £36m in phishing losses were borne by one bank, which rather undermines the incentive for other banks to improve their security. By now, the attacks are more equally distributed, yet the phishing website take-down contractors used by the different banks don't share information with each other, which makes their operations much less effective than they could be [8].

The overall trend in the UK is that the payment services industry is progressively externalising the fraud risk on to customers and merchants. This may seem superficially attractive, but is unsustainable. First, systems cannot remain secure if the principals who guard them do not bear the costs of failure: we see the beginning of this in the rising tide of card fraud and phishing, and in the certification failures referred to above and in [4]. Second, the externalisation of risk on customers and merchants will mean it is managed much less well: the payment service providers are best placed to do risk management as they alone have access to data on billions of transactions from which trends and anomalies can be detected.

If merchants and customers have to manage risk, they will do so in ways that cost the economy much more. For example, customers will use electronic banking services much less than is optimal, resulting in high costs for cheque clearing, call centres and so on. And an example of the likely outcome of dumping all cardholder-not-present risks on the merchant may be seen in South Africa, where it is extremely difficult to acquire CNP transactions from foreign cardholders: some acquirers ask for a fax of the cardholder's credit card and passport. This makes it extremely difficult for South African businesses to operate online unless they have foreign associates for card transaction acquisition.

In short, a more equitable and transparent system of regulation – such as that enjoyed by US bank customers under Regulation E and *Judd* v *Citibank* – is actually in the long-term interests of the payments sector. The present state of affairs is a failure of regulation, and although short-sighted bankers might welcome it, we hope that the Payments Council will take a more intelligent and strategic view.

Answers to specific questions

Q1 asks whether the industry should have a 'proactive' plan to manage the decline in cheques. We believe this needs a broader context. Selfish action by the industry is likely to damage other sectors, and to damage the economy overall. It is unlikely even to be in the long-term interests of payment service providers. Any such plan should be devised at a level where the rights of others will be taken properly into account; this means in practice the UK Government or the European Commission.

Q2 asks for what types of payment currently made by cheque would be need alternatives. The obvious answers are (a) payments where the payer is unwilling to accept a fraud risk

imposed on her by systems over which she has no control and against which she has no effective legal recourse (b) payments made between individual members of the public

Q3 asks whether a target date of 2018 would be acceptable for an end to cheque clearing. In the absence of any evidence that the payment services industry is prepared to embrace the kind of regulation considered normal in the USA, the answer is no.

Q4 asks how to educate users to accept a migration away from cheques. In the absence of regulatory changes, FIPR will oppose such a move and will seek to educate the public to demand that Parliament vetoes it.

We have no comment on questions 5 or 6.

Q7 asks whether we agree to a review of paper credit clearing. The objective here appears to be that bank customers should be compelled to pay utility and other bills electronically rather than in person at bank branches. It therefore raises all the same questions as the abolition of cheques and in the absence of appropriate customer protection we oppose it for the same reason.

Q8–10 ask whether cash will remain a major payment method and how it should be handled. Despite efforts in many countries to get people to use electronic purses such as Proton, Geldkarte, Moneo and the new RFID cards over perhaps 20 years now, these mechanisms have not made major inroads and it is safe to assume that cash will remain. The supply of cash should be left to the Royal Mint and the note issuing banks.

Q11–13 ask whether direct debits could be made available for more purposes, such as one-off payments, and whether some of the liability for wrongful debits (whether erroneous or fraudulent) could be dumped on the accountholder. This is an extremely bad idea. It would make UK direct debits similar to US Automated Clearing House (ACH) payments; yet ACH fraud is growing vigorously, with the result that prudent US accountholders place ACH blocks on their accounts, or limit ACH debits to a list of named counterparties. The idea that anyone who knows my bank account number can debit my account is bad enough; at least, at present, the debiting firm has to guarantee to give back the money should I notice and object. To provide that a careless or fraudulent debiter could get away with it so long as I didn't notice, or didn't object within some short period, would create significant moral hazard.Indeed, we find it somewhat disturbing that the Payments Council even saw fit to include such a question in its consultation.

We have no comments on questions 14–15.

Q16–17 ask what should be done about cash machines, and whether the infrastructure can be exploited to deliver new services. Many banks have experimented with new services in many countries over the past 25 years, from bill payment to vending prepayment utility tokens and mobile phone topups. That none of these gimmicks has become universal should perhaps tell us something; and of course banks should be free to

experiment on the off-chance they eventually come up with a killer app. However the main problem with cash machines is the lack of effective dispute resolution. We believe that the UK (indeed the EU) should adopt the US Regulation E and the reasoning in *Judd* v *Citibank* to ensure that the onus of proof in disputed transaction cases lies squarely on the bank, as a matter of practice as well as a matter of law.

We have no comment on questions 18–20 or 22.

Q 21 asks what improvements should be made to cross-border payments. We believe that asset tracing and recovery should be faster and simpler. This is becoming urgent, as the growth of phishing and of keyloggers will mean that at any time hundreds of UK bank accounts will be under the control of criminals who have taken them over. Experience shows that the best way to deter such attacks is to make it difficult to get away with the money [9]. Irrevocable cross-border payment mechanisms (such as Western Union) are the main phishing hole at present; in the past other mechanisms have been used (such as eGold). Service planners and regulators must ensure that no systemic holes open up that could undermine the resilience of the payment system.

Q22–24 deal with contactless and prepaid cards. Contactless cards as presently deployed use protocols similar to EMV but with many of the security measures removed; they are thus vulnerable to cloning and relay attacks [10]. Many of the consumer protection issues discussed earlier thus arise once more in this new context. It may be thought that PINs can be dispensed with for transactions under £10; but what will be the response when bank customers start complaining about large numbers of small transactions that they do not recognise? The risk here may be exacerbated by the fact that the next generation of mobile phones will implement NFC protocols that will enable them to emulate both cards and terminals. That will be convenient, in that your credit card can become an application on your phone. It will be less convenient when criminals program phones to harvest card data and perform relay attacks. The development of this technology must of course be left to the payment service providers; but the regulatory aspects must not be.

We have no comment on questions 31–36.

Q 37-38 ask about financial inclusion. A recent study of nonbank payments [9] pointed out that the anti-money-laundering regulations imposed since 9/11 have not only been counterproductive in their own terms (by focussing on identity rather than traceability) but have also damaged financial inclusion. For example, poor African farmers also need financial services as part of their path out of poverty, but now find themselves excluded as they cannot show two utility bills to prove their address. (Indeed many don't even have addresses.) The 'identity circus' also has direct costs for people entering the UK banking system for the first time, and harms immigrants and arriving students as well as young people born in Britain. The payments industry appears to welcome the identity circus, perhaps because it increases customer lock-in and perhaps because it enables banks to plead due diligence when a customer turns out to be a crook. This is counterproductive. The industry should set its face against the identity circus and push for its abolition.

Q39 asks `What are the main challenges to the integrity of the payment system that need to be addressed collaboratively?' We have already discussed a number of the main points. First, by throwing liability over the fence, banks ensure that it won't be managed well (or at all). The providers of payment services are much better placed than any other stakeholder to manage payment risk as they alone have access to all the information and they alone can change the systems to minimise it. Second, we believe that the industry is wrong in asking about the 'integrity' of the payments system: in a world in which, at any one time, hundreds (perhaps thousands) of customer accounts have been taken over by criminals via phishing or malware attacks, the real question is the resilience of the payments system [9]. The goal is not to pretend that attacks don't happen – that fools no-one any more – but to identify them rapidly and recover from them at minimum cost to the affected customers. Third, the breakdown of security certification of financial systems – whereby equipment that isn't secure is certified as secure, and no-one's prepared to take any action about it – needs to be fixed.

However, the most important challenge by far is to get the liability right. Britain – and the EU – urgently need to adopt consumer-protection laws along the lines of the US Regulation E and *Judd* v *Citibank*, so that payment service providers cannot externalise liability for security and other failures in their systems. You cannot expect a system to remain secure where the people responsible for maintaining and guarding it do not suffer the financial costs of failure.

Q40–48 ask in more detail about fraud, security and risk allocation. We reiterate that the incorrect allocation of liability in the UK is the fundamental problem. When that is solved, everything else will follow; but so long as it is not solved, purely technical measures are unlikely to give significant relief.

If banks bear liability for their systems, then it can be left to the market to work out what protection mechanisms will be most cost-effective. The arms race between fraudsters and security engineers is extremely rapid: far too fast for regulators to play a useful role at the tactical level. Regulators should concentrate on getting the strategic questions right, such as liability and recourse.

However, since the consultation asks, we are at present somewhat sceptical about CAP; if used in challenge-response mode it's too vulnerable to man-in-the-middle attacks, and if used to authenticate transaction details it's too cumbersome. We suspect that two-channel authentication would be better; a customer attempting to send money to a new payee might get a text message saying something like 'If you really do want to pay $1247 to Hisab Travel in Egypt, please enter 4156 in your browser now'. Such systems have worked better abroad than two-factor.

We are also sceptical of regulators imposing more technical standards, as they are not just likely to be out-of-date (or plain wrong) but are also likely to be used as excuses to deny justice to customers; for egregious examples, see the appendices to our response to the Hunt Review on the Financial Services Ombudsman. The regulator should instead tackle the strategic question of why the existing standards for security evaluation are clearly not

working, as we noted above.

For more detailed technical information on what's wrong with current payment systems and standards, we recommend that the Payments Council read all ten documents cited in the references below – and read them carefully.

Q49 asks whether the Payments Council should 'establish a better understanding of the costs of UK payments'. This is rather ambiguous. If it means 'The Payments Council should undertake a marketing campaign to persuade UK account holders that free banking be brought to an end' then of course we disagree, and such a campaign would make clear that the Payments Council is just another trade lobby group – in which case it's unclear why its functions cannot simply be performed by APACS.

But then the Payments Council's own remit is ambiguous: it describes itself as 'a newly created strategic payments body set up to regulate and represent the payments industry'. If the Council wants to make a serious contribution to the policy debate, then we'd suggest that it collect and publish much more detailed information about the costs and benefits of payment systems, and do so in ways that have greater credibility than the current offerings.

Ross Anderson
Nicholas Bohm
Martyn Thomas
February 4 2008

References

[1] FIPR Submission to the Hunt Review of the Financial Ombudsman Service, at www.fipr.org
[2] N Bohm, I Brown and B Gladman, 'Electronic Commerce: Who Carries the Risk of Fraud?' Journal of Information Law and Technology, October 2000, at http://elj.warwick.ac.uk/jilt/00-3/bohm.html
[3] R Anderson, 'Security Engineering', Wiley, 2001; second edition 2008
[4] S Drimer, S Murdoch, R Anderson, 'Thinking Inside the Box: System-level Failures of Tamper Proofing', at IEEE Symposium on Security and Privacy 2008
[5] R Anderson, T Moore, 'Information Security Economics – and Beyond', Crypto 2007, at www.ross-anderson.com
[6] R Anderson, 'Why Cryptosystems Fail' in Communications of the ACM vol 37 no 11 pp 32–40, at www.ross-anderson.com
[7] H Varian, 'Managing Online Security Risks', New York Times, Jun 1, 2000, at http://people.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html
[8] T Moore, R Clayton, 'The cost of non-cooperation when countering phishing', 2008
[9] R Anderson, 'Closing the Phishing Hole: Fraud, Risk and Nonbanks', Federal Reserve Santa Fe Conference, May 2007, at at www.ross-anderson.com
[10] R Anderson, 'RFID and the Middleman', in Eleventh International Conference on Financial Cryptography and Data Security (Feb 2007), Springer LNCS v 4886 pp 46–49, at www.ross-anderson.com