Closing the Phishing Hole – Fraud, Risk and Nonbanks

Ross Anderson
Professor of Security Engineering
Cambridge University

Abstract

Online fraudsters use a variety of nonbank payment services to launder the proceeds of crime. People had assumed that traceability was the key. However, investigation reveals that revocability is more important. Fraudulent payments within the banking system can be pursued and recovered with a reasonable probability of success; but once stolen funds are used to buy transferable financial assets such as eGold, recovery becomes much harder. This suggests that much of the benefit that could be obtained from regulating nonbanks more closely can be got by greater transparency about counterparty risks. I also look at broader issues; just as adequately regulated offshore financial centres can benefit the global financial system by providing competition, so also nonbank payment systems can play a useful competitive role. A further issue is the confusion between identity and traceability that has crept into compliance procedures since 9/11; I argue that there has been too much emphasis on the former at the expense of the latter. The current FATF rules impose unnecessary burdens, particularly on the poor, while not doing enough to facilitate rapid recovery of stolen assets. Future regulation of nonbank payment services must take account of this. Anonymous or unverified payment mechanisms can be tolerated, particularly for low value instruments, so long as stolen funds can be quickly traced and recovered. One must also be cautious about liability. Many nonbank payment systems use contracts that attempt to make them judge and jury in disputes with customers – risking a race to the bottom that would undermine consumer protection, and moral hazard which exacerbates operational risks. Only payment service providers can fight fraud effectively, as only they have access to all the data, and the ability to evolve their systems. Consumer protection thus cannot be ignored in payment system resilience.

Introduction – fraud and phishing

Since about 2000, there has been a growing realization that the management of information security risks crosses the boundary between technology and policy. Systems often fail not so much for technical reasons, but because incentives were wrong; often the people who operate a system are not the people who suffer the full costs of failure. (Indeed, systems are often designed deliberately to externalise risk.) This has led to the growth of a new discipline of security economics, which now has over 100 active

researchers and two annual conferences[1]. One question asked by the Federal Reserve when asking me to give this talk was: what might a security economist say about online fraud and its associated operational risks in the context of nonbank payment services?[2]

Since about 2004, online crime has become big business. Before then, a typical 'hacker' was a teenage prankster who tried to infect machines or knock out networks to impress his peers; and while there were some online scams, they tended to be sporadic and disconnected. That has now changed. People now write computer viruses not for fun, but for profit. Infected machines are organised by the thousand into botnets that are rented out to send spam, conduct service-denial attacks, and host fraudulent websites. The critical change has been the emergence of an underworld economy, so that villains can specialise and trade with each other.

The most rapidly growing online crime appears to be phishing, in which victims are lured by an email to log on to a website that appears genuine but that actually steals their passwords. It started in 2003, with half-a-dozen reported attacks[3]. These were both crude and greedy; the attackers asked for all sorts of personal information, and even for ATM PINs, which made many customers smell a rat. By 2004 the phishermen had raised their game, using copies of genuine bank emails and websites, and better psychology. By 2006, losses had climbed to £35m in the UK, and nine figures in the USA. Growth continues at a phenomenal rate, with the target list now including not just large banks but also nonbank payment services such as PayPal and large retailers like Amazon.

Although it is easier for crooks to build a copy of a bank's website than it is to build a bogus bank branch in a shopping mall, the infrastructure required for a successful phishing attack is still not entirely trivial. But this is where the growing underground economy is coming into its own. An American software engineer may now write malware used by a Romanian botnet herder to take over thousands of machines; he in turn rents them out to a Russian phisherman who sets up the bogus website and spams the bank's customers. There follows a chase in which money is moved from compromised accounts. These accounts are traded; there are also organisations that recruit 'mules'[4].

So a number of gangs remove money from compromised accounts, pass them through other compromised accounts or mules, and finally move them through a nonbank such as

---

[1] For a recent survey article see 'The Economics of Information Security – A Survey and Open Questions', Ross Anderson, Tyler Moore, Softint 2007 (Jan 19–20, Toulouse); at http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf

[2] Another was 'Will online gambling be the killer app that makes nonbank payments popular?' However, gambling is moving to Second Life, to the point that the FBI raided it: http://www.reuters.com/article/technologyNews/idUSN0327865820070404?

[3] R Clayton, 'Techno-Risk', at Cambridge International Symposium on Economic Crime 2003, at http://www.cl.cam.ac.uk/~rnc1/talks/030910-TechnoRisk.pdf

[4] Mules are often poorly-educated elderly people, recruited by 'work from home' ads, who believe they are earning an honest 10% by remitting funds they receive in their bank accounts onward to an 'exporter' overseas

eGold or Western Union. Finally the stolen money is taken from the payment system by specialist cashout operators, who may belong to another gang entirely. As with Adam Smith's pin factory, specialisation brings the criminals great productivity gains.

There are variants such as 'pharming' in which the deception is not carried out on the customer directly but on the infrastructure; for example, home routers may be taken over and configured to direct bank customers to malicious web pages instead of the real ones.

Much work has been done recently on technical defences against phishing and pharming, but there is a growing realisation that technology can only do so much[5]. First, there is the classic security-economics issue that everyone wants someone else to solve the problem; at a recent UK conference, the government wanted citizens to take more responsibility for their own safety online, while banks blamed the government and the ISPs, and everyone else was eager to distance themselves from the problem in other ways[6]. This liability dumping is endemic; it has been modelled by Hirshleifer and Varian in terms of whether the security of a system is determined by the sum of the defenders' efforts, the maximum effort that any of them makes, or the minimum effort that any of them makes. In the last case the actual defense effort may fall particularly far short of the social optimum[7].

Second, the standard security mechanisms shipped with commodity PCs are not really fit for purpose. The SSL/TLS protocol was designed in the mid-90s to dump compliance costs on users[8], and again, the underlying reason was economic – companies competing for dominance in markets with strong network effects (as Microsoft and Netscape were in the browser market at the time) are motivated to put their complementers' convenience above their customers' security. A competing protocol that would have been more resistant to phishing – SET – was also resisted by the banking industry because of higher infrastructure costs and by consumers as it eliminated chargebacks and dumped liability on them.

Third, banks' marketing departments are often hard to distinguish from phishermen. Perhaps the worst example came from a large high street bank in the UK, which sent out a share-dealing spam with a URL not registered to the bank. Its web page sensibly advised its customers not to reply to emails, click on links or disclose details – and the spam itself had a similar warning at the end. The mother of a student of ours received this spam and contacted the bank's security department, which told her it was a phish. The student 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. When a main-street bank's

---

[5] A recent book is M Jakobsson, S Myers, 'Phishing and Countermeasures'. Wiley 2007

[6] See for example Ross Anderson, 'TK Maxx and banking regulation', at http://www.lightbluetouchpaper.org/2007/03/30/tk-maxx-and-banking-regulation/

[7] See Jack Hirshleifer, 'From weakest-link to best-shot: the voluntary provision of public goods', in Public Choice v 41, (1983) pp 371–386; and Hal Varian, 'System Reliability and Free Riding', in Economics of Information Security, Kluwer 2004 pp 1–15

[8] Don Davis, 'Compliance Defects in Public-Key Cryptography', Proc. 6th Usenix Security Symposium (San Jose, CA, 1996), pp. 171–178

own fraud department can't tell its own spam from phish, what can reasonably be expected of bank customers?[9]

Fourth, the attack technology has a long way to develop. In the latest twist, known as 'vishing', bank customers are told to ring a bank call centre that is actually run by the crooks. Their voice-response software is programmed with not just the same scripts that the genuine service uses, but even the same voices. Designing usable security that not only enables banks to recognise genuine customers, but customers to recognise genuine banks, is seriously hard. And there will also remain issues with the security of the underlying platform. Here again economics matter; Windows Vista makes huge efforts to protect premium video content, but almost no effort to protect users' credit card numbers.

For all these reasons, it is unreasonable to expect that the integrity of the payment system can rest on front-end authentication mechanisms alone. It will have to be assumed that, at any time, a proportion of customer accounts will be under the control of malefactors. Back-end controls will be vital: to limit the exposure, to detect fraud in progress, to slow down transaction velocity, and to recover stolen funds quickly. At the philosophical level, we may need a shift of emphasis from the 'integrity of the payments system' to its resilience. The old system withstood occasional dishonest insiders who tried to steal large amounts of money, and mostly failed. Occasional dishonest insiders still exist; but we now also have large numbers of compromised customer accounts, and we have to ensure that the payment system will withstand them too.

Fraud controls and how they fail

The first consumer e-banking system, fielded in the 1984 by the Bank of Scotland, had very strict use controls: customers could move money between accounts, but make third-party payments only to accounts they had previously nominated in writing. Thus to pay an electricity bill, a customer would have to visit her bank branch and fill out a form with her electricity company, her customer number and a monthly payment limit. Needless to say, there was little fraud. So the controls were gradually relaxed, and then mostly swept away in the enthusiasm of the dotcom bubble.

In addition to institutional controls, there are system-wide controls. Banks have long cooperated in recovering money stolen by fraudsters. For example, if a programmer inserted an unauthorised transaction into the SWIFT message queue, commanding a payment to an accomplice overseas, then hopefully the bank's balancing procedures would pick up the anomaly the following business day, whereupon a senior manager would call a contact at the recipient bank and arrange for the accomplice to be arrested when he showed up to collect the cash. The few successful scams found some way to extract value from the banking system; in the notorious Security Pacific case, Rifkin used a wire transfer to buy diamonds from a Russian broker, while in a case known to the author the perpetrators set up a loan guarantee for a shell company.

---

[9] SA Mathieson. 'Gone phishing in Halifax – UK bank sends out marketing email which its own staff identify as a fake'', Infosecurity News, Oct 7 2005

The SWIFT and wire frauds that we worried about 20 years ago have now been industrialised, and the banking industry has to industrialise the means of coping with them. In the last three years, the flood of phishing attacks has caused asset recovery arrangements to be put on a production-line basis in the UK. Rather than requiring senior management intervention, transaction reversals are initiated by front-line staff in bank fraud departments, backed up by a network of cross-indemnities between banks.

The critical questions here are whether the banking system is responding properly to the stress imposed by phishing, and more generally whether it can evolve appropriately in response to novel threats[10]. Security economics teaches that this will depend in large measure on whether the incentives are properly aligned.

In the UK, one single bank took £30m of the £35m phishing losses sustained in 2006. According to investigators, the phishermen target this bank because of its lax internal controls, and above all its poor record of asset recovery: apparently it recovers only about 60% of stolen money compared with 75–95% for its competitors. I do not have hard figures for the USA but anecdotal evidence from the investigator community suggests a similar pattern: rapidly rising fraud, with losses concentrated on banks that subject their online customers to fewer controls and that have less effective asset recovery teams.

In the last two years, the phishermen have switched en masse to nonbank payment systems such as eGold (with Western Union trailing in second place). It was initially thought that this was due to eGold's offshore status, and the difficulty of using subpoenas to disclose the destination of stolen money. However, in the past year (since a raid, IRS action against its parent company, pressure over child porn sites and a stream of subpoenas[11]), eGold has become responsive. There has been some displacement of business, notably to Webmoney[12] and apparently to banks in the Baltic states from which transfers to Russia are easy, yet eGold remains the cut-out of choice.

According to investigators, the real attraction is that eGold payments are not revocable. Although policemen trying to trace child-porn website operators or money launderers can now get information from them, asset recovery operators have so far been unable to recover stolen funds transmitted through their system. For organised criminals, traceability a few months after the fact is of little relevance; in many jurisdictions, they can get people with forged (or even genuine but corruptly-issued ID) to turn up and collect the cash, while even within the best-regulated countries they have no difficulty finding disposable persons such as drug addicts to do the cashout and take the rap later.

---

[10] A key insight of the new field of systems biology is that robustness is evolvability; see H Kitano, 'Self-extending symbiosis', Biological Theory 1(1) 2006 pp 61–66

[11] B Grow, J Cady, S Rutledge, D Polek, 'Gold Rush', Business Week, Jan 9 2006; at http://www.businessweek.com/magazine/content/06_02/b3966094.htm

[12] B Grow, B MacWilliams, 'WebMoney and its Customers', Business Week, Jan 9 2006; at http://www.businessweek.com/magazine/content/06_02/b3966104.htm

The phishermen's goal in selecting a cut-out is not so much to conceal the identity of low-grade cashout operatives, but rather to frustrate bank fraud departments by slowing down the process of asset recovery.

Implications for bank regulation

In the familiar world of paper-based banking, a cheque (or other bill of exchange) could be dishonoured if insufficient funds were available, or if funds apparently available turned out to have been the proceeds of fraud (as in kites, bust-outs and similar scams). Incoming payments were treated as uncleared effects for some time, and could be revoked even after that. Risk-management mechanisms evolved at a number of levels; in the UK, different banks had different rules for treating assets as uncleared (from three to ten days' delay). London's merchant banks made money for centuries by 'accepting' (guaranteeing) bills of exchange issued by merchants. The markets managed the risk well; in effect the risk ended up with the most capable trust service providers.

Last time I bought a car, I paid my bank £40 for a bank draft (cashier's check) which insured the car dealer against the possibility that my cheque might bounce – perhaps even after the clearing window, if it turned out to be drawn on evil funds. The market allocated this particular risk to my bank; as I have been a customer there for over 20 years, they can probably write such insurance business more cheaply than anyone else.

However, during the wave of innovation unleashed by the dotcom boom, we have seen the emergence of intermediaries who in effect sell cashiers' checks below market, because they have managed to insulate themselves (using offshore status) against the effects of people buying their scrip with stolen money. If this continues, then quite apart from its effects on crime, it will disrupt the existing markets for risk; if eGold can sell you a cashier's check for £20 when Lloyds' Bank charges £40, then people will use eGold to buy their cars and the market for cashiers' checks will dry up.

Maintaining the resilience of the financial system depends on allocating risks to those parties best able to deal with them. If this can be done transparently by market mechanisms, so much the better; then the initial allocation of risks will at least be less critical. However if the market fails and each principal seeks to dump liability on others, then there can be a race to the bottom in which trust is lost.

How can we ensure that the system of electronic payments remains resilient, as the paper-based system did for many years? In a world where any retail banking payment may have been ordered without the mandate of the accountholder – and a small but significant number will have been – the natural strategy for the regulator is to insist that by default all electronic payments ordered by individual accountholders should be considered provisional until enough time has passed for the affected parties to have received and checked their bank statements (at least 90 days – PayPal uses 180).

Provisional payments will suffice for the great majority of low-value transactions between individuals, and between businesses that deal with each other frequently. There will of course be a market demand for irrevocable instruments – 'digital cashier's checks'. Quite possibly, for small amounts and good customers, irrevocable payment will only entail a small amount of extra hassle (such as answering a confirmation SMS message from one's bank) so long as the credit risk is supported by an automated assessment and the payee is of good standing. Transfers to low-value systems such as e-purses may be free. But most likely, guaranteed payments to entities that are known to be conduits for financial flight will carry a heavy premium; and guarantees will cost even more for real-time payment than for next-day settlement. This will create an incentive for nonbank payment operators to know, and police, their customers much more effectively.

Implications for competition

There is an interesting parallel between nonbank payment services and offshore financial centres, of which a relevant survey appeared recently in The Economist[13]. Offshore centres can be a worry not just because of criminal finance but also because of tax evasion and the systemic risks from large unregulated financial flows, where esoteric derivatives make risk less transparent. However, the competition they provide on the tax, regulatory and service fronts help prevent large-country governments from getting bloated and inefficient, and also provide a competitive spur to conventional financial centres.

Nonbank payment systems can similarly provide useful competition to their regulated counterparts. In the 1990s, as Internet shopping was getting under way, credit card companies made exorbitant charges in many countries; small businesses in the UK were at one time being charged merchant discounts as high as 8%, and the card transaction acquisition business was the target of competition and fair-trading enquiries. Even large businesses were paying over 2%. It might have been thought that this was a reasonable premium for the card system accepting counterparty risks through the system of chargebacks, but there was also a move by UK banks to disclaim liability where overseas merchants failed to deliver goods of merchantable quality or at all.

Given that such oligopolistic practices posed a potentially serious threat to the development of e-commerce, the arrival of nonbank payment service providers such as PayPal was timely. PayPal's later takeover by eBay was also instructive; given eBay's reputation systems, there were available synergies in that a payment service linked to eBay could provide counterparty guarantees more efficiently than the typical card-issuing or -acquiring bank.

Another example comes from phone-based payments; the MTN MobileMoney system in South Africa was developed by MTN, a mobile phone service provider, and provides rapid phone-based payments at a fraction of the cost of cheques or wire transfers. This is good news for the country's rapidly urbanising population, many of whom are unbanked

[13] J Ramos, 'Places in the Sun', The Economist, Feb 22nd 2007

and may not even have street addresses. (In this case, the system is operated under an agency agreement with an established bank, which provides the regulatory cover.)

The emergence of payment companies linked to technology firms is nothing new. Western Union was founded in 1851 as a telegraph company, linked the US West and East coasts ten years later, introduced the stock ticker in 1866 and started a money transfer service in 1871. By the end of the 19th century it had become mostly a financial services company. Even though the established banks were early and heavy users of the telegraph, they could not beat a technology company at service innovation[14].

Of course, nonbank payment services are not limited to Western Union and to its Internet successors such as PayPal and eGold. Hawala, hundi, fei chien and other traditional payment systems have been in use for generations; before 9/11 they offered serious price competition to the existing banking system, with a $5000 transfer from New York to Islamabad costing $5–10. On November 7th 2001, the President of the US declared that informal value transfer systems had to be placed under the microscope to prevent flows of funds related to terrorism or crime; the Patriot Act (s373) cracked down on unlicensed money transmission businesses, and since then, pressures to implement anti-money-laundering controls have pushed the price up to roughly the $100 that the conventional banking system charges. (This seems to have been bad for competition: by 2002, the level of expatriate remittances from the USA to Pakistan through the regulated banking system had doubled.) The UK also took simultaneous (if less drastic) action, requiring money remitters to register with HM Customs from November 12th 2001.

Scholars of the hawala system now express reservations about the effectiveness of heavy-handed regulation, arguing that a light touch that keeps the operators' support and trust leads to better law-enforcement outcomes[15]. For example, hawala operators keep long-term records in Western countries where their operations are legal, but destroy them post-settlement in South Asia where their business is outlawed. India, which criminalised hawala in 1973, downgraded the prohibition to a civil matter in 2000; and Pakistan, which previously enforced a bank monopoly on payment services, has said that some hawala operators will be licensed. (Hawala operators are actually better at transaction tracing and revocation than many critics believe, but both of them depend on records being retained.)

Alternative payment systems do not have to be either traditional or web-based, and indeed mechanisms will be improvised where they are needed. A good example is found in the Democratic Republic of the Congo, where following the collapse of the governmental and commercial infrastructure people started using prepaid phone cards as currency. When gangsters take a hostage in Katanga, they may get his family in Kinshasa to pay the ransom by buying $50 worth of phone cards and texting them the codes.

---

[14] T Standage, 'The Victorian Internet', Walker and Company, 1998

[15] N Passas, 'Informal Value Transfer Systems, Terrorism and Money Laundering', US DoJ report 208301, January 2005

In countries that do have functioning banking systems, their interface with the informal sector is critical for regulation. Conventional wire transfers and negotiable instruments are widely used to settle aggregated nonbank payments, which gives some useful leverage to regulators. PayPal is very open about the fact that it 'leverages' the banking system: it's used to 'verify' account holders by sending a small amount of money to their bank account, whereupon the account holder must confirm that she controls that account by reporting the amount and the payment reference back to PayPal. In this way PayPal avoids the tiresome collection of millions of customers' utility bills. MTN does something similar; customers can operate accounts on the basis of a claimed identity subject to balance and velocity limits, and have these limits removed by showing up at a bank branch with an ID document and proof of address.

We can therefore expect there to continue to be a mix of nonbank payment systems. Some will be traditional, some technology-driven, and some ad-hoc. The broad regulatory goal should be the same as with offshore financial centres: to get the competitive benefits of alternative systems while preventing them being too easily exploited for crime. To quote The Economist:

> Two decades ago, they were mainly passive repositories of the cash of large companies, rich individuals and rogues. Some jurisdictions still ply this trade today and should be put out of business. But the best of them—for example, Jersey and Bermuda—have become sophisticated, well-run financial centres in their own right, with expertise in certain niches such as insurance or structured finance.
>
> This special report will argue that although international initiatives aimed at reducing financial crime are welcome, the broader concern over OFCs is overblown. Well-run jurisdictions of all sorts, whether nominally on- or offshore, are good for the global financial system.

The key questions are what sort of rules we should seek to impose on nonbank payment services, and how we can go about imposing them in a globalised world. I've already argued that traceability of payments, and in particular the revocability of unauthorised payments, are critical. I'll now look at issues such as privacy, identity and consumer protection.

Tracing money, or tracking people?

Providing anonymity to honest customers is not fundamentally in conflict with the rapid tracing and recovery of stolen funds. Digital-cash-type systems can handle traceability fine – you need a database of recent transactions anyway to foil double spending[16]. (The electronic coins invented by Chaum and promoted by his company Digicash are seen by many engineers as the 'proper' way to do e-cash, but their deployment has so far been held up by patent issues – which will go away as the Chaum patents expire.) There have

[16] D Chaum, 'Achieving Electronic Privacy', Scientific American, August 1992, pp 96–101, at http://www.chaum.com/articles/Achieving_Electronic_Privacy.htm

been many publications on how anonymity can be made conditional in such systems, so that an accountholder's identity is revealed if he or she commits a crime[17].

The ad-hoc way in which anonymity was provided by eGold and some others – transferable accounts that were at best loosely bound to real-life identities – raises more interesting issues. Traditional bankers believed it was important to 'know your customer'; London bankers would insist on personal references, while their counterparts in Zürich would want to see a passport – even if the account itself was presented to the outside world as an anonymous 'numbered' one.

Since 9/11 there has been a strong law-enforcement focus on identity rather than money. There was a US push to furnish all humans with government-issue photo ID. This has provoked hostility even among the staunchest of US allies. Britain's Conservative Party plans to fight (and looks like it will win) the next election on a platform that includes opposing the planned ID card, while a Home Office survey reveals that 15 million people may refuse to get one[18]. In the USA itself, the effectiveness of the US-VISIT program has been repeatedly questioned[19].

Thanks to pressure from the Financial Action Task Force (FATF), bank customers worldwide have become familiar with an 'identity circus' over the last few years – where even private bankers feel driven to write to customers of thirty years' standing asking them for utility bills as proof of address. This is not merely ridiculous, as private bankers know their customers far better than the gas company does; it is a classic example of risk management having been displaced by due diligence, which in turn creates moral hazard. A corrupt bank manager may reckon he can get away with opening accounts for a money launderer so long as he has a bundle of gas bills filed away. Gas bills are easy enough for the wicked to forge, especially now that the UK has over 400 gas companies, many of which supply bills online. But the regulations are oppressive to many groups of law-abiding people, such as married women whose household bills are addressed to their husbands, and students arriving at university from overseas. The worst hit are people in the third world; there are millions of people living in huts in Africa with no addresses and no utilities but who need financial services as part of their route out of poverty.

The old methods were also in many ways more effective. When I first opened a bank account I needed references from two existing bank account holders. The online world is at last rediscovering benefits of 'social networks' as they are now called.; social networks can be mapped and suspicious patterns of relationships detected. A too rigid approach to identifying customers has thus led to a serviceable system being replaced by one that is easier for criminals to fool.

---

[17] R Davies, 'Electronic Money, or E-money, and Digital Cash', at http://www.ex.ac.uk/~RDavies/arian/emoney.html

[18] R Winnett, D Leppard, 'Millions to rebel over ID cards', Sunday Times Apr 8th 2007, at http://www.timesonline.co.uk/tol/news/uk/article1626768.ece

[19] see for example EPIC, 'United States Visitor and Immigrant Status Indicator Technology', at http://www.epic.org/privacy/us-visit/

So the push for identity is running out of steam politically and is becoming relatively ineffective in developed countries, where better mechanisms are available. In the developing world it is worse, as ID documents tend to be nonexistent or corrupt. People in India do not generally possess ID; and while they do in Pakistan, it is easy to get ID documents in false names by bribing officials. The Pakistan problem is so bad that the UAE set up an iris-recognition system at its ports and airports to check the identities of arriving passengers against a database of deported persons (many of them prostitutes from Pakistan). So far over 73,000 passengers have been found to be on the watch list[20].

The push for ID also harms some established nonbank payment services directly; for example, Western Union has tried hard to get ID from payment recipients, but has taken reputational damage in Nigeria and elsewhere after people turned up to collect funds using bogus IDs that may have been issued for the purpose by corrupt officials[21].

Now that five years have passed since the post-9/11 regulatory push, it is time to stand back and assess what was overdone and what was underdone. ID is running out of steam and is no longer believed to be a panacea. However, the existing framework does not sufficiently mandate timely cooperation in asset recovery. The closest in FATF's 25 criteria is that each country or territory must criminalise the laundering of the proceeds of serious crimes, and in any case the FATF campaign has come to a natural conclusion with all countries except Myanmar now compliant[22]. However, the theft by a phisherman of $4000 from a customer account may not of itself be deemed a serious crime. The closest in its 40 recommendations is no. 38, that '*There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value*.' Again, it might be argued that phishing isn't money laundering, and 'expeditious' can be interpreted in some countries as weeks to months, rather than hours. So I am unable to agree with the 2006 FATF report that its rules are adequate for new payment methods[23].

The underlying problem may be that we have let banking regulation be driven by law-enforcement concerns, strategies and tactics. In fact economics are fundamental.

Not only is crime correlated with economics – it falls as countries get richer – but even in the domain of civil conflict and terrorism, economics are a key driver. Groundbreaking research by Paul Collier and Anke Hoeffler for the World Bank examined whether civil

---

[20] J Daugman, 'United Arab Emirates Deployment of Iris Recognition', at http://www.cl.cam.ac.uk/~jgd1000/deployments.html
[21] N Passas, *op. cit.*
[22] FATF, 'Annual Review of Non-Cooperative Countries and Territories', 2005–6
[23] FATF, 'Report on New Payment Methods', October 13th 2006

wars are driven by greed or by grievance[24]. The data overwhelmingly support an economic cause. Grievances are easy enough to find or manufacture; but for a civil war to be sustained, there must be some way for the combatants to be paid and supplied. We can see the roots of the Irish conflict in the willingness of Irish-Americans to donate to the IRA, while the Sri Lankan civil war was fueled by donations from Tamils in the USA, India and the UK. (The Irish war ceased, and the Sri Lankan war became quiescent for a while, after 9/11 dramatically lowered US tolerance of terrorism.) And insofar as Islamist terrorism is still financed by wealthy but misguided donors in the Arabian peninsula, tracing money matters there too, at least as much as tracing people. We have to redress the balance between the two. Financial transparency and traceability matter a lot more than collecting easily forged copies of gas bills.

It may be instructive to note that PayPal is relaxed about ID, though it limits what 'unverified' users can do, keeps payments provisional in principle for 180 days, and does not let customers withdraw cash in 'send-only regions' – countries with poor regulation and law enforcement.

Implications for money laundering controls

At present, financial institutions bear considerable compliance costs in relation to money laundering, and the controls are largely focussed towards the input end – the pizza parlours or other places where cash is fed into the banking system. There is relatively little attention paid to the layering process, where money is moved from one account to another, or to the output process, where bank-system credit is turned once more into unregistered assets (although interest in the latter phases has been growing recently).

Phishing compels us to pay attention to output. Any mechanism that enables a wire transfer to be turned into portable wealth can be used to break the asset-recovery chain and is thus likely to be used by the online crooks sooner or later.

Making payment and counterparty risk transparent will thus help move the focus in money laundering control from the input stage to a more balanced view of input and output. We may also expect that properly-designed revocation mechanisms will make tracing easier too, making the layering process more accessible to investigators.

A shift in emphasis from tracing people to tracing money also makes sense in the context of the growing global movement to recover the proceeds of crime generally, not just online crime. In 2000, the UK had a government report on 'Recovering the Proceeds of Crime'[25]; this led to the Proceeds of Crime Act in 2002, which set up the Asset Recovery

---

[24] Anke Hoeffler, Paul Collier, 'Greed and Grievance in Civil Wars', 2004, Oxford Economic Papers 56: 663-595; see also 'Breaking the Conflict Trap: Civil War and Development Policy', OUP 2003

[25] UK Cabinet Office, 'Recovering the Proceeds of Crime', at www.cabinetoffice.gov.uk/strategy/downloads/su/criminal/crime.pdf

Agency. The ARA's goal is, first, to seize money from convicted criminals; second, where a prosecution has failed but an action for civil recovery might succeed against an offender under the lower standards of proof, to mount a recovery action; and where criminals are resident in the UK to assess them for tax on the proceeds of crime.

The idea is good, but so far it's not working for fraud. Most of the £14m asset freezes done by 2004 related to drugs; yet the ARA estimates that the UK's three most profitable criminal businesses are fraud (losses and costs of £14bn), illegal drugs (£6.6bn) and vehicle thefts (£900m)[26]. On these figures, asset recovery from fraudsters remains rather disappointing. Shifting the emphasis from slow traceability to rapid revocability can only help. Our proposal would limit irrevocable payments to large, explicitly-guaranteed payments (such as cashier's checks) where the markets would create pressure for the underwriters to know their customers, and to low-value systems such as e-purses and phone payments with limited scope for abuse in laundering the proceeds of fraud.

Customer rights

One obstacle to recovering the proceeds of crime is where the losses fall on people who do not have the resources to conduct recovery operations. A particularly worrying trend in this regard is the move by banks in Europe to dump the liability for fraud on customers and merchants. This started many years ago when the rules for ATM fraud diverged on the two sides of the Atlantic. In the USA, the first 'phantom withdrawal' case was decided in favour of the customer[27], leading to Regulation E and its limits on customer liability for unauthorised transactions. In the UK, initial cases went the other way; banks got away for years with claiming 'our systems are secure so if your PIN was used it's your fault'. This created the obvious moral hazard, leading banks to be careless about ATM security, and ultimately an avalanche of ATM fraud in 1992–4 which forced a revision of the UK Banking Code.

One might have thought that liability dumping would have given UK banks a competitive advantage over US banks, whether by spending less money on security or on suffering less fraud. This turned out to be wrong. British banks spent more money on security, as they were doing due diligence rather than risk reduction, and ended up suffering more fraud because of the moral hazard. This curious anomaly was one of the sparks that kindled the initial interest in the economics of information security[28].

The theory is being tested experimentally. After UK banks introduced EMV 'chip and PIN' smartcards two years ago they returned to the 'infallibility' doctrine and started refusing customer complaints; the predictable ramp-up in fraud has already begun. The banks have also dumped liability for cardholder-not-present fraud on the merchants.

---

[26] J Earl, 'The Work of the Assets Recovery Agency', NAO Fraud conference, at www.nao.org.uk/conferences/fraud/ConferenceSlides.pdf

[27] Judd v Citibank, 435 NYS, 2d series, pp 210–212, 107 Misc.2d 526

[28] Hal R. Varian, 'Managing Online Security Risks', New York Times, Jun 1, 2000; at http://www.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html

More recently, the move to electronic banking led many financial institutions to impose terms and conditions on their customers that once more dumped the fraud risk; customers who accepted a password for use in telephone or online banking thereby accepted that the burden of proof in disputes shifted to them. The different banks' terms were analysed by Bohm, Brown and Gladman[29]. The 'Verified by VISA' program now seeks to make online payments to merchants fall under these terms; in effect the cardholder-not-present fraud risk will be transferred from merchants to issuers and on to customers.

The most recent example of liability dumping is the proposed EU Payment Services Directive[30]. This would effectively level down consumer protection in Europe to the lowestcommon denominator, namely that in the UK. Banks will be able to set dispute resolution procedures by their terms and conditions and thus effectively act as judges in payment disputes. It is yet to be seen whether the European Parliament will amend this before it becomes law, but Europe's banking industry is much more concentrated than America's, and has in the past been all too effective at lobbying.

How does all this concern the US regulator, and in the context of nonbank payment services? Quite simply, nonbanks have an incentive to arbitrage risk, which leads them to dump liability along the European model. The classic is eGold: if your passphrase was used you're liable, all spends are presumed authorised, and no payments can be reversed[31]. The least objectionable appears to be PayPal, whose user agreement for US customers specifies alternative dispute resolution under $10,000 and otherwise litigation in California (with attorney's fees paid by the winner); its agreement for EU customers specifies using the UK courts or Financial Ombudsman Service (the former expensive and the latter notoriously pro-bank). To be fair, PayPal does proclaim that it always makes good customer losses due to unauthorised transactions, and in many ways it is a model service provider. However if PayPal mistakenly thought a customer had colluded, and the customer wanted redress, this could turn out to be more difficult than with a bank.

It seems inevitable that as more and more payment services are deployed that are vulnerable to online fraud, the constant factor will be a stream of complaints from honest citizens that 'I didn't do that' or 'I was cheated into doing that – I thought I was paying $2 for a parking meter in Baltimore and here I'm being billed $2000 for casino chips in Macao'. The contentious technologies will also change – the headline issue might be ACH scams this year, and RFID transaction forwarding in five years' time[32]. But there must be robust means of dealing with customer complaints; otherwise not only will confidence be lost, but the incentives needed to track down wrongdoers and to improve

---

[29] N Bohm, I Brown, B Gladman 'Electronic Commerce: Who Carries the Risk of Fraud?' JILT 2000 (3)

[30] Proposal for a Directive on Payment Services (PSD), at http://ec.europa.eu/internal_market/payments/framework/index_en.htm

[31] eGold, Terms of Use, at http://www.e-gold.com/unsecure/terms.htm

[32] RJ Anderson, 'RFID and the Middleman', Financial Cryptography 2007, at www.cl.cam.ac.uk/~rja14/Papers/rfid-fc07.pdf

systems will be suboptimal. Ultimately, it's only the providers of payment services who can fight fraud; only they have access to all the data, and the ability to evolve the system. If the banks (and nonbanks) don't take the pain, they won't take the strain.

Conclusions

Human societies have always had laws to make it hard for a thief to get away with stolen goods or money. In general, a thief could never acquire good title to his victim's goods. There were some rules to create certainty about ownership: in medieval England, if you stole my horse and sold it to the vicar at an open regulated market between dusk and dawn, the vicar acquired good title to the animal. (This did not extinguish my right to have you hanged and seize the money back from your estate.) Laundering money was harder; apart from a few arcane special cases[33], stolen money could always in principle be recovered.

For this reason, transactions needing certainty of payment have long used intermediaries who insured the counterparty risk, be they accepting houses who underwrote merchants' bills, factors who would discount invoices without recourse, or bankers who sold cashiers' checks to their customers. So long as such risks were transparent and transferable, the market allocated them to the principals best able to bear them, which usually meant a financial institution to which the relying party was well known. This apparatus of risk management was largely unanalysed, except in rather general terms by law-and-econnomics scholars, and never really became a formal part of bank regulation.

Over the last ten years, the growth of electronic payment services has undermined this. Rapid globalisation has created strong incentives for principals to throw risks over the fence; regulatory confusion and arbitrage have led financial institutions to rewrite their contracts to dump risk on their customers (whether cardholders or merchants) whenever they could; and new nonbank payment schemes have been set up outside traditional regulatory frameworks. While some of these new payment services have been operated in good faith by large, reputable companies, others have cut corners – and even the best have shaved away at traditional consumer protections. Third-party arbitration is being replaced with an approach of 'trust us – we will refund you if you're defrauded'. This risks a return to the world of early eighteenth-century banking regulation, a race to the bottom, and perhaps even an electronic South Sea Bubble.

Regulators' initial reaction to the problem has been confounded by the sequelae of 9/11 and in particular the drive to issue people with biometrically-linked government-issue photo-ID. Regardless of the costs and benefits of this program, it has been implemented at the cost of regulators taking their eye off the need to trace stolen funds. Following the money and naming the suspect are not perfect substitutes, and this shift has serious costs. Now that the ID push is running out of steam worldwide, we need to move the emphasis back to following the money.

---

[33] Such as when an exchange-control fraudster fled to a country without exchange controls and sheltered behind dual-criminality provisions

A further issue is the move in many countries (notably in Europe) to shift liability for unauthorised transactions from the relying party to the party alleged to have done the authorisation. The EU draft Payment Services Directive will in particular challenge Regulation E, which has served the US banking industry and its customers well for a generation. The risk is that by shifting fraud liability from banks to merchants and customers, asset recovery efforts will be undermined, together with the incentives to keep payment systems secure.

In conclusion, I suggest regulators think seriously about the revocability of electronic payments. Clear rules in the USA would have the potential to propagate outwards to the better-regulated countries (including well-regulated offshore financial centres), as payments to countries with inadequate controls would have to be irrevocable payments and would thus attract a risk premium. This would make nonbanks less attractive as vehicles for financial flight; if eGold accepted only cashiers' checks, the phishermen would not use it much.

It appears to be in this context that the most rapid progress can be made towards a light-touch regulation of nonbank payment system operators that will preserve and foster competition, uphold consumer rights, protect the payments system against contagion, and above all enable us to adapt to a new age: an age in which the emphasis will shift from protecting the integrity of the payments system, to ensuring its resilience in the face of attack.

Acknowledgements: I have had useful discussions with a number of people including Richard Clayton, Nick Bohm, Steven Murdoch, Johann Bezuidenhoudt, Matthew Pemble, Nikos Passas, Sharon Lemon, Andy Auld, Keith Mularski and Rafal Rohozinski. The writing of this paper has, thanks to them, been an unusually educative project.