

Card tricks

Cardholder not present (CNP) fraud is growing fast. Thanks to the effectiveness of chip and PIN at the PoS, the fraudsters have moved online. However, Penelope Ody finds retailers are fighting back

According to APACS, in the 12 months to April 2007 CNP fraud in the UK leapt by 47 per cent. In 2006 it reached almost £213 million and has continued to climb steadily during 2007. Today, CNP fraud now accounts for more than half of all fraud involving UK issued cards and there can be few of us who have not experienced – or known someone first hand who has – a fraudulent attack on our cards through CNP.

"There is significant growth here," says Martin Lewis, operations manager for APACS Cards and Fraud Control unit. "Magstripe data is easily stolen and shipped off for use overseas or in CNP."

It is, it seems, a surprisingly easy and highly lucrative form of theft. At the Retail Fraud conference held in London in May, 'T', a convicted fraudster, took the stage with Martin Gill, professor of criminology at Leicester University, to be interviewed about his tactics. They were very, very simple. As a cash-strapped student, 'T'

had friends working part-time in call centres who – for little more than the price of a few beers – willingly passed over card numbers, names, addresses and telephone numbers of the callers. 'T' then simply rang the prospects and very easily extracted such vital information as mother's maiden name, date of birth or whatever other answers to security questions the glib fraudster asked.

Armed with the information, "T" changed the cardholder's address details and shopped online for anything saleable, filching thousands of pounds from each victim before the fraud was identified and he moved on to the next prospect.

'T' – now reformed – is probably a minor player: a lone operator with a few well-placed friends. Most CNP fraud is rather more organised and much bigger business – a global crime network with key hotspots in Eastern Europe. It is also an area where the basic anti-fraud precautions are all too frequently ignored. While the latest CyberSource survey of online retailers suggests that around

70 per cent of merchants use address verification service (AVS) and card verification number (CVS) to authenticate online transactions, less than half use either



fraud and loss prevention supplement | CNP fraud



MasterCard SecureCode or Verified by Visa, just over a third use fraud screens, only 29 per cent bother with industry hot card files and under a quarter use IP geolocation checks.

Form filling

Both SecureCard and Verified by Visa have been actively promoted in the past year but take-up still appears slow – even though there is a 30 June deadline from MasterCard for only accepting Maestro cards protected by the technology. A possible deterrent for customers is that the online application form, with its requests for security identifiers, looks rather like a phishing attack to those less familiar with such things.

“Banks in other countries have opted for partly completed pop up forms,” says Mark McMurtrie, director of marketing at The Logic Group. “Here they haven’t and that can deter sign up. It’s been rather a chicken and egg situation – not enough people enrolling to make it work adopting these systems and not enough sites offering the service to make it worthwhile adopting. Integrated IT systems capable of delivering a partly completed form could have helped.”

Obviously retailers want to sell goods and too many barriers to payment will cut conversion rates still further. However, all too many have poor processes which make it easy for the fraudster to succeed. Identity check specialist 192.com has established the Prove-ID fraud forum to allow retailers to openly discuss fraud experiences and share best practice to help improve processes and cut fraud losses. Its ‘top five giveaways’, which suggest that despite apparently good authentication the transaction could be fraudulent, are:

1. The retailer receives a post-order as well as a pre-fulfilment telephone call from the customer requesting a change of delivery address.
2. A low value order ‘test purchase’ is immediately followed by a high value order.
3. The cardholder address is more than 50 miles from the delivery address.
4. The order comes from a known fraud hotspot, which according to 192.com includes such areas as London SE28, Estonia and Nigeria.
5. The order is placed using a free email address that bears little resemblance to the customer’s name.

“The issue with many retailers is that they are not using the data they have available to them,” says Bart Patrick, head of risk strategy at SAS UK. “Most counter-fraud strategies are focused on physical detection and prevention. What is missing is the use of predictive analytics which provides the ability to model fraud and predict, in a statistical manner, fraudulent activities, stopping them before they actually happen. Only by catching fraud prior to the event will companies eradicate financial loss.”

Fair Isaacs, for example, sells detection systems based on customer usage profiling and neural network models. Its Falcon fraud management tools are widely used by the banks – resulting in those out-of-hours telephone calls asking you to confirm that you really did draw a large sum of cash at the airport or

make some other out of character purchase. Although a retail version of the system has been available for several years there are, so far, very few users.

"CNP losses are down to the merchant not the bank," says Peter Bove, client partner at Fair Isaacs, "but if retailers put in more robust authentication tools they could argue that losses really should be down to the banks – as they are with fully authenticated chip and PIN."

Bove points out that it can already be difficult for a fraud victim to prove that they did not undertake a fraudulent PIN-authenticated transaction as the banks have tended to argue that "it was your PIN, it must have been you". A similar attitude could develop with CNP fraud once the current trend for a second positive ID becomes more commonplace.

Authentic solutions

Various techniques – from one-time password code generators and online chip and PIN devices to fingerprint ID – are now being trialled for online transactions. Pay by Touch, for example, has launched TrueMe which uses fingerprint ID to enable online transactions. Shoppers can use a plug-in USB reader to authenticate their fingerprints and encrypt details for onward transmission. Fingerprint ID is already used with some laptops, largely for access security, but take-up for online shopping appears to be slow.

Mobile telephones, too, are being used for authentication. Sybase has just launched securePay which uses a cardholder's mobile phone to verify the transaction in real-time.

The various second factor authentication techniques may seem infallible but mobile phones and secure password generators are easily lost or stolen and it is not that difficult, or unknown, for fraudsters to hack into sites and change biometric identifiers to match their own iris images or other details. Shoppers will also inevitably forget to carry around their one-time passcode generators when travelling or away from their usual PC or desk.

"These sorts of devices are being used to provide secure access to Internet banking," says The Logic Group's McMurtrie. "They're not – so far – intended for shopping. If they prove successful then perhaps we'll see wider use, but that could be at least three years away and will involve a great deal of commercial agreements and standardisation as well."

As McMurtrie points out, none of us wants a separate passcode generator for each site we access or each card we use, and many of us use payment cards from a number of financial service providers – not just our main bank. Either the banks all agree and share the costs of providing a common platform or consumers will end up having to buy their own standard gizmo – something which many will be reluctant to do.

Second factor ID can make it extremely difficult for a

genuine customer to prove that he or she did not authorise a particular transaction. It can also lull retailers and banks into a false sense of security. "We had one US bank which installed dual factor authentication for online banking," says Fair Isaacs' Bove, "and they thought that was enough – so once the fraudster was past that hurdle it was easy and they were very badly hit indeed."

An additional concern is a growing trend for customers to see online transactions as high risk. Excessive security and transactions denied are an irritation – as are aggravated encounters with banks or merchants trying to claim payment for dubiously fraudulent purchases. McMurtrie cites a recent Ipsos-Mori poll which suggests that 90 per cent of consumers are now worried about online security.

PCI:DSS compliance will certainly improve cardholder data security and avoid TK Maxx-style débâcles, but will do little to stop 'T' and his accomplices using rather more devious means to extract vital data from gullible consumers. Perhaps what we need is not just smarter technology but greater consumer education and improved processes. Next time your bank telephones with a new product offer and asks you to answer a few security questions first – ask *them* to prove who they are before answering.

