

Chip and PIN – biggest UK retail project since decimalisation, but not enough on its own to defeat card fraud

Philip Hunter

The credit card industry's big idea for tackling fraud, chip and PIN, is being rolled out in earnest within the UK, but security experts warn that on its own it will merely divert criminals to other channels. Chip and PIN does nothing to address cardholder not present (CNP) fraud, notably for online purchases over the Internet, and still leaves the door open for fraudulent transactions from identify theft.

Chip and PIN should indeed virtually eliminate fraudulent transactions within retail outlets using stolen or counterfeit credit or debit cards, but will not stop criminals obtaining cards using stolen names, addresses and other personal details. Such cards would still work because the fraudsters would be issued with authorised cards and PINs.

Even in the pre chip and PIN era, both CNP fraud and identity theft have been proliferating, although the former did slow down markedly in 2003. CNP fraud in the UK increased 6% from 2002 to 2003 to £116.4 million, while fraud resulting from obtaining credit cards using stolen credentials, ie identity theft, went up 45% to £29.7 million over the same period, according to the Association of Payment Clearing Services. Both the police and the security industry have warned that the advent of chip and PIN will boost these frauds and in particular reinvigorate the CNP field as criminals switch to online activities.

The chip and PIN project is the biggest retail logistical exercise since decimalisation in the late 1960s, involving the roll out of 143 million cards to 42 million people, along with upgrades to 850 000 retail terminals and 40 000 cash machines. It also entails transfer of liability for fraudulent transactions from banks

to retailers, so in a sense it had better be secure or a number of merchants will go out of business. Certainly many small retailers are both confused and worried by the prospect, and a number plan to retain dual functionality and continue supporting conventional signature customer verification for some time, diluting the security benefits.

Chip and PIN does nothing to address cardholder not present (CNP) fraud

There is even some concern that the much-trumpeted security of chip and PIN at the point of sale could be compromised to some extent by a concerted effort from fraudsters. The main risks concern the PINs themselves, should it be possible to obtain access to those, and the ability of criminals to reprogram the chips of stolen cards. The knowledge required to reprogram chips, and the hardware to do so, are already available on the Internet. The point is that the PINs are stored not on the central back end system, whose operation is unchanged by chip and PIN, but on the smartcard. This avoids the risk of PINs

being eavesdropped in transit, but does mean that security depends on the smart card's memory being inviolable.

Certainly a large scale fraud involving chip and PIN chips in the early days, should it occur through no fault of retailers, could terminally damage the technology's reputation and acceptance. It is fair to say that no such fraud is anticipated, and that the loopholes such as they are will be difficult to exploit in the short term at least, being well beyond the scope of the sort of criminal involved currently in conventional credit card theft. And the industry is convinced that chip and PIN will make a huge impact on counterfeit card fraud, which totalled £148.5 million in 2002, along with stolen card fraud, at £108.3 million in 2002.

Whether this will happen will not be known for sure until the cards are deployed not just in the UK but internationally so that they can be used around the world. The UK roll out is due to be finished by January 2005, making the country the first to have a retail infrastructure fully compliant with the global EMV standard for interaction between the chip and smartcard reader. Other leading industrialised nations are expected to swiftly follow, so just as happened with magnetic swipe cards, chip and PIN will quickly become ubiquitous.

But this still begs the awkward questions of dealing with CNP and identity fraud. The expectation at the turn of the Millennium was that by now the majority of PCs would be equipped with smartcard readers, which would at least enable chip and PIN protection for online CNP transactions. There is still some hope that this will be happen eventually, perhaps taking off once everyone has a chip and PIN card anyway by next year.

But this is not certain and so other avenues are still being pursued, notably Address Verification, Security Code Checking, and the twin Verified by Visa and MasterCard SecureCode schemes, all of which have already been used to varying degrees. Address Verification tackles theft of credit card details for online transactions by matching the street

number and postcode entered with an order with the record of the legitimate cardholder held on file by a bank. This however has the effect of blocking a number of legitimate transactions. Retailers are therefore given the option of allowing through transactions flagged as failing address verification. Alternatively a retailer can take note and conduct its own verification checks, perhaps involving a phone call and checking additional security information. In general retailers can reduce their exposure to online fraud through a few relatively straightforward almost commonsensical measures, such as declining orders originating from free, Web-based or email forwarding addresses, and also orders that come without contact phone numbers. Larger retailers can automate this checking and also install intelligent software to identify those orders that have a whiff of potential fraud. These can then be checked – the point is that there is a window between initially accepting orders and finally closing the transaction, even if customers are not aware of this. The window can be used to turn the spotlight on a subset of orders identified as being potentially fraudulent.

Security code checking, involving the three additional check digits on the back of credit cards, is increasingly used to

reduce fraud associated with theft not of the card itself but of the card number and name of the holder as can be gained from receipts. This has had some success, but does not help in the event of the card itself being stolen, nor for eavesdropping of transactions or hacking into customer databases.

To guard against credit card theft, if not necessarily against hacking of customer details, the only recourses are either to private information known only to the customer, ie a password or PIN – or some biometric. An obvious candidate would be the PIN issued with the emerging chip and PIN cards, but the Internet is not deemed secure enough to transmit PIN numbers, leaving the possibility as already noted of doing it via smartcard readers in the same way as at the point of sale. However Verified with Visa and MasterCard Secure Card provides an immediate solution based on passwords. When users enter credit card details at the online checkout of a Web store enrolled in the programme, a window pops up asking them for the password. However this has an administrative overhead, and requires customers to remember a password in addition to their PIN.

This leaves that old can of worms, biometrics. While the most promising candidate is iris recognition, even this, quite

apart from problems of user acceptance and costs of deployment, suffers from too great an incidence of both false negatives and positives. It appears that acceptable accuracy could at present only be obtained at an unacceptable cost and burden upon the user by combining two methods such as fingerprint and iris recognition. The chance of somebody being falsely recognized on two independent biometrics is greatly reduced.

However serious consideration has been given to the use of photographs at the point of sale, as an alternative or adjunct to chip and PIN. Indeed Citibank offers credit cards embossed with photographs as an option, rather like the modern driving licences, and has already reported a 67% reduction in fraud incidence among customers who have taken this up. But this is largely because of the disincentive effect, for the quality of the photographs is often inadequate for confident identification. An alternative is to have higher quality images stored in digital form in the card's memory, but this would require costly display devices at the point of sale. As a result the industry has decided to run with chip and PIN, but while this seems likely to be successful at eliminating some fraud at the point of sale, it will only shift it to the Internet unless there is a consistent approach at that level.

Confidential data theft and loss: stopping the leaks

Stephen Hinde, Bupa
It wasn't me, it was the virus

First we had "it's a computer error" now we seem to be blaming errors on computer viruses. During the last year we have seen computer viruses blamed for problems in education, democracy, courts and law enforcement.

..... a virus ate my exam results

The West Bengal Education Minister blamed a computer virus for students receiving incorrect marks in Higher Secondary examinations. He told the State

Assembly in Calcutta, India that an unnamed computer virus attacked computer systems, resulting in a number of errors on mark sheets. 19 separate cases of irregularities in marking were discovered, and blamed on virus infection. The fact that this was not the first time the examination

results have been found to be in error may indicate that the unnamed computer virus was innocent of the allegations!

..... US democracy held up by computer virus

The counting of votes in Will County, Illinois, USA was disrupted by a computer virus. Some precincts, which electronically transmit results to a central server, were unable to do so because this server was flooded with bogus requests as a result of a virus infection. The website designed to publish election results as they came in crashed during the attack, denying voters and candidates the actual election results. The Director of Information Systems said