

Preventing Card-Not-Present Fraud



by **Bea Havier**
Fraud Expert – The 3rd Man

Every day there seems to be a new solution that provides a miraculous answer to the problem of (CNP)fraud. Bea Havier takes a look.

We all know that CNP fraud is something that retailers in particular need to take steps to detect and prevent, but the problem must be kept in perspective. Many retailers already comfortably manage the threat and do so with little or no impact on their genuine and honest customers.

Some of the latest solutions such as 3D-Secure, which requires a password to authorise transactions, or Token-Based Authentication, which challenges the cardholder to input another passcode generated by a hand-held gismo, are being promoted heavily.

But unless fraudsters choose to use the new security measures, they will only impact genuine customers.

Pointing the finger

Unless of course the solutions are mandated. Mandated by the banks who have a track record in using the Interchange mechanism – the way the banks agree the fees payable to other banks – who, no doubt, will be delighted to see the new measures adopted, irrespective of the impact they may have on genuine customers.

After all, this is not so much about preventing fraud as it is about shifting blame – and there have been precedents. Take Chip and PIN for example. On February 13th 2006, if a card was swiped in a store and a signature obtained at the time of authorisation, then the majority of the risk lay with the card issuer. After Feb 14th, fraudsters were offered the opportunity of huge reward if they obtained information from the credit card together with a PIN. This opportunity has proven to be very popular in some areas. Now that Chip and PIN has been mandated, the real issue is that risk of fraud lies with either the retailer or the cardholder, not the bank. The marketing department at the bank has done a great job: most people still think Chip and PIN is safer, which it is – for the banks.

Internet security

In e-commerce, a similar scenario is playing out with Verified by Visa and Mastercard Securecode. If a cardholder authenticates a transaction, then the blame is with the cardholder. If a transaction is not authenticated then the blame lies with the retailer, not the bank. The key here is that the cardholder who had virtually no liability with CNP fraud will now be at threat if password or authentication details are compromised – and that is exactly what the fraudsters will seek to do.

Furthermore the key to preventing CNP fraud lies with the retailers who now will only care about receiving fully authenticated orders.

But there is a sting in the tail for the retailer too!

If a fully authenticated transaction was made using compromised details, then the genuine cardholder will query the transaction in due course. The bank will say that it was fully authenticated, and the cardholder will argue that no goods were ever received. In the event that goods are not delivered, this will be charged back to the retailer, just like it is today!

“So what has changed?” I hear you say. The answer is that if it is not the retailer’s fault then it is the cardholder’s!

Dynamic passcode authentication

The newer, dynamic passcode authentication is a much stronger solution all round, as it is more difficult to compromise the authentication process. The weakness here is that the solution relies on 100% adoption, and as long as there are banks who do not support it, or cardholders who don’t have one of the little gizmos, then retailers will still need to make judgement calls, just like they do today.

So we are addressing a problem which many retailers cope with just fine at present, and we are using new technology that will impact the shopping experience of all our genuine customers but very few fraudsters. What is needed is a campaign to encourage fraudsters to use the new security measures.

Bank led initiatives are all useful in preventing fraud. However the justification to implement must be made based on the discounted rates that the banks have agreed to give retailers as inducements. Negotiate a better fee on the basis of improved security. Retailers must remember that alone these measures will not solve CNP fraud. Keep updating your fraud screening techniques – or better still rely on companies such as the 3rd Man to do it for you!

