

When the chips are down....

The advent of the use of Smart Cards in the card payments industry has been heralded by many, including this author, as one of the biggest steps towards decreasing the amount of credit and debit card fraud.

The implementation of this technology has meant that merchants, card issuers and cardholders could be assured now that the person in possession of the credit/debit card is the rightful owner.

While the implementation of Chip and PIN is quite recent in Ireland, it has been commonplace for many of our European neighbours for many years, particularly in the Debit card area.

The principle is that there is a computer chip inserted in the plastic of the credit/debit card and there are a number of terminal contact points that allow a reader access the information stored on the device. This information can only be accessed once the user has entered the secret numeric code, the PIN (Personal Identification Number).

The reason that this has added so much extra security to the payment card transactions is that it is technically very challenging, not impossible, to forge these devices. One of the bugbears of the Payment Card Industry (PCI) has been the ease with which the magnetic strips on the back of the previous generation cards could be cloned. These magnetic strips still exist on the back on the Chip and PIN cards, but are there for legacy purposes and to identify that this is a Chip and PIN card.

The practise of cloning, or "skimming" credit cards has been huge business for the fraudsters over the years, and the source of serious losses for the PCI. In Ireland, there was a large skimming operation uncovered based on staff in bars and restaurants in the popular tourist areas in Dublin. The staff were supplied with cigarette packet sized devices that they kept in their pockets. Each time a customer gave them a credit/debit card, they "skimmed" the card through the device and the critical information was recorded. This information was then downloaded to computers at a manufacturing line in a warehouse in West Dublin and thousands of counterfeit cards were produced. This sort of operation should not now be possible as the use of Chip and PIN spreads.

However, in the recent weeks, a scandal concerning the integrity of the Chip and PIN process has started unfolding.

It appears that a number of the largest banks in the United States of America have been re-issuing hundreds of thousands of cards to their customers. They have also been preventing PIN based ATM withdrawals from accounts of all their customers in certain countries around the world until this issue has been addressed.

Why these banks have felt compelled to take such drastic action has not been fully disclosed, but is widely believed to be as a result of a massive breach of customer PINs at retailer sites.

Many would believe that when using a Chip and PIN terminal to authorise a particular transaction that there would be no copy of the PIN entered stored anywhere. However, this has not been the case in some of the Point of Sale equipment in the retailers at which these breaches are alleged to have occurred. Some Point of Sale equipment stores the PIN and the Terminal ID from which the transaction occurred in

encrypted databases. However, if these were to be breached, it is the gold at the end of the rainbow for the fraudster. The magnetic stripe information for these cards is often also stored in these databases and that means that the fraudster now has all the information necessary to perform unauthorised ATM withdrawals from the customer account. Hence the disabling of all ATM withdrawals in certain countries where these fraudsters are suspected of operating.

How can such a breach occur? Firstly, it is a very poor development process for any Point of Sale organisation to record and store the PINs of customers performing Chip and PIN transactions. In fact, the Payment Card Industry has a set of development standards that specifically prohibit this practise. This is not of much comfort to those that have been a victim of the fraudsters, or inconvenienced by their actions as the banks restrict their services. In recent days, Visa has informed the media that it is investigating a specific international supplier of software in the area of Point of Sale solutions for the prohibited storing of customer card information, up to and including PINs.

In the future, compliance with the PCI standards, and being tested against their policies and requirements will be a competitive advantage for financial institutions, merchants and the developers of Point of Sale solutions.

At the end of the day, it is the consumer that will end up paying for the cost of this fraud. This is because the issuing banks in most cases will make good on the fraud that is not the user's direct responsibility. Credit and Debit card users must take some responsibility in this battle with the fraudsters and adhere to a few basic principles when using their cards. These include shredding statements and receipts rather than just throwing them in the bin, never let your card out of your sight when in a restaurant/bar etc, do not use your card details for age or address verification on the Internet and only provide card details to online merchants that state they are compliant with the PCI standards.