

banking technology

HOME ANALYSIS COMMUNITY AWARDS DIRECTORY OF SERVICES INDUSTRY RESOURCES
News Company Announcements Email Bulletin Free Sample

Comments

04 January 2010

text-size: [+] [-] [RESET] [BACK]

TechBrief: A view from the crow's nest

Jonathan Hancock, TSYS

The issue of fraud, and in particular data compromise, is very topical at the moment. Recent events in Spain involving a major card processor that connects most of the country's automatic teller machine and point of sale networks has acted as yet another wake-up call to everyone in the card issuing, acquiring and processing sector. The fact that an apparently secure network was compromised was considered serious enough for both Visa and MasterCard to release bulletins advising that card issuers should take appropriate action to protect their cardholders' data. Forensic investigations into how security was breached and exactly what information has been compromised are ongoing, and the results will be used to improve security across the globe and to prevent similar occurrences in the future.

Unfortunately, despite the tight security currently in place, data compromises appear to be happening more and more frequently. Long gone are the days where fraudsters would simply pick-pocket an individual in order to steal a single card. There is also less evidence of the once prevalent practise of fraudsters setting up camp in a restaurant and skimming diners' card's as they come to pay at the end of a meal. The challenges that the industry is facing today are much more organised, much more complex and much more sophisticated. The fraudsters are clearly organised, well funded and technically astute. They know what they are doing and they are targeting very large organisations with the intent to steal cardholder information. Fraudsters have certainly moved up the value chain to a position where the act of committing the fraud is that much harder to perpetrate, but the rewards are that much greater. One of the downsides of the growth of global data systems and the Internet is that many of these data compromises can be perpetrated remotely. Fraudsters working from thousands of miles away can hack into a system and steal the information remotely while hiding their tracks every effectively.

In order to reduce the risk of security breaches and fraud, and promote best practice, the Payment Card Industry Data Security Standard has been widely adopted. PCI DSS sets out guidelines on how to protect and what to protect in the payments industry. Most large processing organisations, TSYS included, are audited against the PCI DSS standard to ensure that security is maintained at the highest level. However there are still many organisations that have vulnerabilities and these are exactly what the fraudsters are identifying and leveraging. The industry needs to look to these vulnerabilities and ensure that they are addressed.

A prime example of what can be achieved when the whole industry adopts a single standard can be seen with EMV, or Chip and PIN as it is better known. The standard was developed by Europay, Mastercard and Visa as a platform to secure the future of payments and has been hugely successful since the first version of EMV standard was published in 1995. The move away from the magnetic stripe to an integrated circuit chip is almost complete, with 99.8% of cards in the UK and 62% in Europe now EMV enabled. The increased cost of issuing a chip card was far outweighed by the long term savings made thanks to the reduced levels of fraud. EMV had a huge impact on reducing counterfeit and lost & stolen card fraud compared with the previous generation of magnetic stripe cards.

The first EMV cards issued in 1999 had a simple static data chip that held cardholder information which could be transmitted across the network to provide authentication. The PIN was then used to verify that the transaction was genuine. The static data chip has now been developed into a more sophisticated dynamic data authentication chip where there are codes within the information that change each time a transaction is made. These codes are then checked against the central host system to prevent cloning or any other form of tampering. If the codes don't synchronise for any reason, the transactions can be flagged and investigated as to whether they are genuine. The card schemes have now mandated that as of 1st January 2010, issuers should migrate their cards onto the dynamic data authentication chip. As a major processor of EMV transactions, TSYS encourages its issuers to migrate onto the new platform as soon as practicable to secure transactions even further. TSYS fully supports the dynamic data authentication chip and will ensure a seamless switchover without any changes or enhancements.

The next evolution of EMV is a combined data authentication chip that uses elements of both previous versions to deliver an even more secure authentication and verification platform.

Having come up against a huge barrier in card present EMV transactions, fraudsters have moved into the card not present (CNP) environment riding the boom in e-commerce. As a consequence, CNP fraud has rocketed and systems have been developed to secure this area of card usage. In the CNP environment, we supports 3-D Secure, the generic name for Verified by Visa and MasterCard SecureCode. This security solution adds an additional authentication step for online payments, usually a password chosen by the cardholder. Further security enhancements can be deployed on the 3-D Secure platform including only asking the card holder for specific characters from the password rather than the whole string. The use of elements of the master password prevents fraudsters from using key-logging software to steal the whole thing.

Another challenging area of fraud prevention is the battle against phishing. Elements of social engineering including fake emails and websites are being used to steal security information from legitimate customers. The customer, having recognised the branding on the email and the look of the webpage, feels confident in entering their security details. Unfortunately the page is not controlled by the bank and all the data being input is being harvested by the fraudsters. The data will subsequently be used to steal either directly from the account or using credit or debit card details associated with the account. Banks and card issuers are continuing to take major steps to combat phishing and some have gone as far as to introduce dynamic passcode devices which using a cardholders chip and PIN card generate a one time use security code that cannot be reused by fraudsters if harvested, making this form of phishing obsolete. But, yet again, not all banks have deployed this level of security and many still use a static username and password that can be reused if compromised.

Identity theft is another form of fraud that is starting to rear its ugly head again. The fraudsters' favourite tactic was 'bin diving' - looking for specific financial information such as discarded bank statements and PIN numbers but also less specific information such as dates of birth, address and mothers maiden name that can all be used to impersonate a legitimate card or account holder. Fraudsters often use this information to contact a bank and request a change of address and shortly afterwards request a new card and PIN number to be sent to the new address. However, following lengthy education campaigns by banks and card issuers most people became aware of the risks associated with throwing away sensitive documents and started shredding their statements.

With a new raft of security measures and best practise in place it is becoming even more difficult for fraudsters to perpetrate this form of identify theft. Banks are starting to use more sophisticated questions not just relying on easily accessible data such as date of birth or mother's maiden name. Details of the cardholder's last transaction are now widely used as a far more secure way of authenticating the cardholder's identity.

Fraudsters have now changed their tactics and having obtained basic information about a cardholder are starting to telephone cardholders claiming to be from the bank and ask for confirmation of key security questions such as mother's maiden name, date of birth and credit limit often quoting the data protection act to give a veneer of authenticity.

There is no silver bullet to solve the problem of identity theft, it is more a case of the banks and the card issuers being vigilant, continuing to educate card and account holders and making sure that they are one step ahead of the identity thieves. TSYS already deploys systems that automatically detect and flag suspicious patterns of behaviour involving changes of address and requests for new cards or PINs using a rule built into the card platform to try and detect account takeovers.

While fraud is still a major problem for the banking and card issuing community, recent initiatives have clearly demonstrated that deploying best practice solutions across the board and focusing on addressing weak points can be highly effective. The use of advanced technology hand-in-hand with the continued educating of cardholders has proved to be a very effective mix. Fraudsters will always try to gain the upper hand in the battle for control, but the banks and card issuers are in a very strong position to protect their interests.

Jonathan Hancock is senior consultant for Fraud Management at TSYS.