

Preventing Card Fraud is More Effective Than Curing It



The banking industry is undergoing a tumultuous period. As the market deals with the ongoing repercussions of the U.S. sub-prime mortgage market crisis and a lack of customer confidence, security also continues to remain high on the agenda for many banks looking to protect their brands and enhance customer loyalty and trust. Card fraud and, in particular, card skimming is just one aspect of security that some of Europe's banks still need to fully address.

As the more innovative banks have found, technology identifying the so-called "point of compromise" (POC) is an important consideration in the fight against card fraud. It is now acknowledged that POC identification must be more widely adopted and should be accorded greater importance.

POC detection is the most important preventive fraud action a financial institution can take when addressing card fraud. The POC is the location at which the card skimming — the illegal copying of card data and PINs for the purpose of stealing money from bank accounts — has taken place. The POC always refers to the specific terminal where skimming occurred; if skimming took place on multiple terminals within a merchant location, then it is said that multiple POCs occurred within the same location.

In 2006, 4,571 reported card skimming attacks in Europe resulted in total losses of just over €305 million for Europe's banks. In order to counter this growing trend, the ideal scenario would be for banks to have the ability to identify cards in their portfolios that are at risk of fraudulent exploitation and take action before any loss has occurred.

This scenario is not hypothetical: The solutions currently exist for banks to take control and beat the card fraudsters at their own game.

Identifying the Point of Compromise

Identification of the POC is important, since it allows financial institutions to recognise trends and write rules based on the type of locations where the compromises are occurring. However, the true significance of the POC approach is only apparent when it is used to identify potential fraud early enough to enable the bank to take preventive action on cards at risk before any money has been lost. If POC detection is used in this way, then such countermeasures can reduce a financial institution's loss per incident by more than 50 percent with little effort.

In order for a bank to identify a POC, it must have available a sufficient number of cards that have experienced confirmed counterfeit fraudulent transactions. The fewer cards, the more difficult it is to identify the fraudulent location with certainty, but a POC can generally be found with as few as two or three cards. The cards used fraudulently provide invaluable information about spending history, and a common point of purchase of genuine transactions across all cards should start to emerge.

It is important to note that the transactions that determine the common point of purchase always occur before the first fraudulent transaction, and all cards should have been used at the same location and terminal within a similar time frame. The further apart the purchase dates, the less likely that this is the true POC.

¹ European ATM Crime Report, The European ATM Security Team (EAST)

Preventing Card Fraud

Found a Match — Now What?

After a common location and time frame have been identified across a number of cards, it is essential to determine other cardholders who may potentially be at risk through the use of the “skimming window.” The skimming window is the period of time between the earliest and latest transactions at the POC on the cards. As more cards are found to carry fraudulent transactions, the skimming window may grow larger. Once a skimming window has been identified, the bank’s transaction database is queried to find a list of all cards that were used at the specific merchant terminal between the dates identified.

Once a list of cards at risk has been collected, a course of action must be decided upon. At this stage, banks often struggle with balancing customer impact against fraud prevention. Unfortunately, the more action relating to fraud prevention that a bank takes, the more customers it will impact. However, there are a number of options open to banks with varying degrees of impact. Depending on the location of the POC, the bank may choose to block cards at risk, monitor or watch cards at risk, do nothing, or perform a combination of the two.

If the location identified as the POC is a high-risk merchant chain where confirmed POCs are a regular occurrence, then the bank may decide that blocking and reissuing the cards warrants the customer impact. On the other hand, if the POC is not known to be high-risk, or there are not enough cards involved to be absolutely certain, a bank may choose to put a watch on the cards at risk. Consequently, any new activity on the card will be flagged as suspicious and alerted to the fraud team.

The Right Tool for the Job

The techniques a bank uses to curtail the impact of fraud can have an enormous effect on its fraud losses. On the downside,

these techniques can also affect staff workload. Identifying POCs and taking action on large numbers of cards using manual processes is time-consuming and difficult.

The only way to properly identify and deal with POC is with a risk management tool designed with POCs in mind. A comprehensive risk management solution with built-in POC functionality is one possible solution. Through the solution’s standard interface, users can access alerts automatically identified and generated by the system when it finds a probable POC. The POC and a list of at-risk cards are displayed for the user to analyse.

Once analysts decide on a course of action, the system allows them to quickly take action on one or many of the cards. With a few clicks, users can place watches on the cards they believe are not a great risk, and they can block cards they believe are high-risk. The system automatically places cards to be watched on a list that can be referenced when writing rules. The more powerful solutions can also examine merchant fraud. As a result, confirmed fraudulent merchant locations can be fed back into the issuer system to automatically identify cards at risk. The ability to introduce countermeasures based on accurate fraud trend data is key to combatting future card fraud.

Financial institutions currently face a number of challenges. Security — particularly card fraud — is only one of these challenges but one that banks recognise as key to their long-term competitive goals. Banks will always have to play a balancing act between customer impact and fraud prevention, but as the old adage goes, “prevention is better than cure.” Europe’s banks will need to increasingly adopt this way of thinking when it comes to their security strategies if they are to retain and regain customer trust and loyalty.