Fraud

New detection method for debit card fraud

Eric Luijks
General manager risk management
Equens

Each year banks lose millions of euros through payment fraud. Equens wants to offer its clients a helping hand by providing advanced services that actively combat this problem. Speed is key in limiting losses resulting from payment fraud. The earlier a bank is aware of possible fraud, the quicker it can take action. Despite the many technical facilities in place for combating misuse of credit cards and debit cards, criminals sometimes still manage to strike.

In the active monitoring of payment fraud, a long-standing successful partnership between Equens and the VU University Amsterdam is bearing fruit – this time to minimise the impact of skimming fraud. This process has been aided by the latest advancements in computer technology, which allow large quantities of data to be matched extremely quickly to show deviations in cardholders' spending patterns.
Equens and the VU University's Fraud detection expertise centre have been collaborating in this field for fifteen years. Bert Kersten, professor of mathematics at the VU University: "Equens had already made major advancements in the detection of credit card fraud. The methodology for detecting skimming fraud is supplementary and highly innovative."

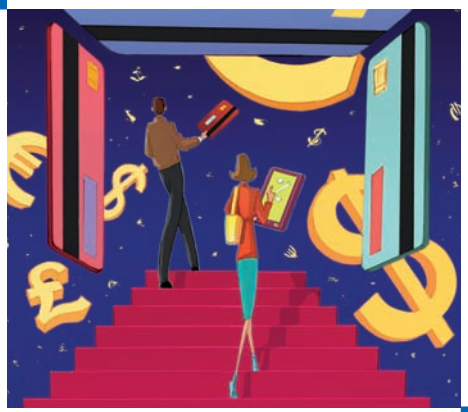
Striking a balance between losses and inconvenience. Banks can authorise Equens to take various actions. For example, Equens can temporarily block a card and, after the block has been lifted, continuously monitor the transactions performed with the card, or advise the bank to take further action. The action to be taken is determined by weighing up the cost and inconvenience to the bank and client. Immediate blocking in the event of the slightest doubt is certainly the safest option, but this would disrupt the operations of the bank and frustrate clients, eventually resulting in costs and perhaps even reputation damage. However, not blocking also costs money. Either way, some form of action always needs to be taken. Concerning the type of action, banks can make individual agreements with Equens and issue them specific authorisations.

Plans for further roll-out in Europe. Fortunately, when compared to payment volumes the financial losses resulting from

skimming are extremely small. Nevertheless, in the Netherlands alone these losses still amount to tens of millions of euros, and in 2009 they increased even more than in the years before. Consequently, skimming fraud needs to be tackled seriously. In the Netherlands, Equens has been employing a system for over a year which, among other things, utilises neural networks. This latest weapon against fraud is based on decades of experience in the area of risk management, and exposes fraud extremely quickly. By acting instantaneously, Equens reduces the amount of time fraudsters have to use the data copied from the cards, making skimming a less attractive proposition. The method was developed for the Netherlands, but Equens now has plans to introduce it in other European countries. Equens and the VU University Amsterdam are considering patenting their latest solution. Considering Equens' leading position in the European payments industry, this will significantly benefit its clients.

Difference between credit and debit card fraud risk.
Credit card fraud is always committed against individual cardholders. In order to detect fraud, individual profiles are matched with the profiles of the transaction and the merchant. If a transaction does not fit the profile, this can indicate fraud. A cardholder discovered this when he went to a jeweller to purchase a piece of jewellery for his wife. Because this was the first time he had made such a purchase, the detection system identified the transaction as suspicious and blocked his credit card. Unlike attempts at credit card fraud, which focus on individual cardholders, skimming focusses on groups. On just one terminal, 50 to 100 cards can be skimmed relatively quickly. Consequently, the methods for fraud detection have been extended with rules for analysing group behaviour.
As a service to the banks, Equens has been monitoring the behaviour of skimmers for years and providing the banks with the information it collects. Bert Kersten says: "This information is extremely effective. Thanks to the rules that have been incorporated, the system relatively rarely makes a wrong decision. Equens' fraud analysts know how criminals work, and we have extensive knowledge of the mining of large data streams. It is real teamwork. You can't do this on your own."

Immediate blocking in the event of the slightest doubt is certainly the safest option, but this would disrupt the operations of the bank and frustrate clients, eventually resulting in costs and perhaps even reputation damage. However, not blocking also costs money.



System detects, human decides. In order to avoid false alarms, it is always a human being – in this case an employee of Equens – who assesses whether an alert is justified or not, and whether action is necessary. Nevertheless, the occasional false positive does slip through the net. For the detection system, a cash withdrawal in Sofia and a payment in the Netherlands made on the same morning using the same debit card represent a deviation from the pattern. However, it is possible. This happened to a businessman who stopped for petrol on his way to Schiphol airport to catch a flight to Guatemala.

When the businessman arrived in Guatemala and made a cash withdrawal at an ATM, his card was blocked. However, when two people make separate payments at different restaurants, but at close intervals, and then each make large cash withdrawals at ATMs in Barcelona an hour later, someone has very clearly been made a victim of card fraud. The system is able to detect fraudulent activities of this nature, and considerably refined attempts, because for every billion transactions, Equens fraud analysts can now compare all transactions from the last few minutes to all previous transactions. These kinds of analyses are performed continuously. "However, this demands considerable processing capacity", says VU University researcher and fraud scientist Dr Wojtek Kowalczyk. "And with mathematical calculations you can determine fairly accurately whether or not something constitutes fraud."

"Due to the speed required, real-time monitoring can only be performed with an extremely large and very fast memory, which is 1 million times faster than a hard disk. This allows us to search very rapidly for unusual patterns in 1 billion of the most recent transactions."

Real-time analysis on the horizon. The current system uses 1 billion of the most recent transactions as a reference for detecting skimming fraud in batches of transactions arriving at fixed intervals.

However, Equens expects to switch to real-time processing of a continuous stream of incoming transactions at the end of 2010. The proof of concept showed that with 24/7 monitoring, immediate losses could be reduced by 70 to 80%, but this needs to be proven definitively in actual practice with real-time fraud detection. "Due to the speed required, real-time monitoring can only be performed with an extremely large and very fast memory, which is 1 million times faster than a hard disk. This allows us to search very rapidly for unusual patterns in 1 billion of the most recent transactions", says Dr Kowalczyk.

Number of skimming cases falling. Equens wants to start tackling payment fraud at the European level. This is fully in line with the pan-European processing strategy. Furthermore, card fraud affects banks across the whole of Europe. The results of tests performed with the new detection system in the Netherlands over a period of one year are very impressive: almost every compromised terminal has been detected.

Cards are also being blocked more quickly than before. More importantly, the number of skimming attempts fell significantly in the first quarter of 2010. Naturally, banks are also taking other measures, but the effectiveness of the fraud detection system is definitely playing a role. This approach will not be able to stop skimming as such, but intervenes so rapidly and effectively that the "business case" will become significantly less appealing for criminals who have to make increasingly large investments in professional equipment to be able to compete with the security levels of ATMs and point of sales terminals. In order to offset the costs, effort and risks, fraud attempts need to be organised on a large scale, which increases the likelihood of detection. In short, skimming is becoming less and less profitable. ■

The results of tests performed with the new detection system in the Netherlands over a period of one year are very impressive: almost every compromised terminal has been detected.