Take charge: Protect your business against card-based fraud

Prevention is better than cure when it comes to card-based fraud, explains **Angelo Bertini,** Managing Director for Middle East and North Africa at BPC Banking Technologies at the changing retail vertical

The UAE experiences the highest rates of card-based fraud anywhere in the world; 44 per cent, as per a study released last year on international and regional card fraud trends. Meanwhile, industry estimates place the total worldwide cost of fraud at more than a whopping $10 billion per annum; the intensification of the e-commerce boom is only hiking this number further up.

And let's not forget, on top of the direct financial costs associated with card-based fraud, the financial institution in question has to grapple with the inevitable hit to its reputation in the marketplace.

Unsurprisingly, card-based fraud severely erodes consumer confidence in providers; 63 per cent of global consumers responding to the aforementioned study claimed they were less likely to use their card after fraud – this further emphasises the negative impact of card-based fraud on businesses, and consequently, the value of being on guard 24x7.

Let's start with the basics: the region's financial institutions need to have in place prevention, detection and response strategies, customised to their zone of operation; card fraud in the UAE, and in turn the Middle East, is not homogeneous. For instance, the level of all fraudulent attacks on cardholders (including ATM and online attacks) in Saudi Arabia is much lower when compared to the rest of the region. These differences are not just observed regionally, but also periodically; a cyclical trend often observed in the industry is financial institutions report a marked increase in online fraud during the holiday period.

The best solution, of course, is fraud prevention. This is a basic, but multifaceted answer to the problem. To begin with, cardholders themselves need to be made aware of methods of safeguard against fraudulent attacks. Globally, 50 per cent of all consumers exhibit behaviour that puts them at a higher risk for financial fraud. Alarmingly, 17 per cent of cardholders in the UAE still make a note of their pin numbers and carry it alongside their debit or credit cards. Obviously, financial institutions need to create awareness on the pitfalls of behaviours such as this.

The provider, on the other hand, needs to be just as vigilant. Examining the system from first principles – the credit and debit cards themselves must be difficult to clone or copy. Next, the payment devices must be protected against unauthorised access, the telecommunications infrastructure must prevent interception and man-in-the-middle-type attacks, and the transaction processing systems – both hardware and software – must be protected against intrusion and manipulation.

> “Industry estimates place the total worldwide cost of fraud at more than a whopping $10 billion per annum”

Moving further from prevention and detection, let's look at response strategies. Once card-based fraud has taken place, the best way to cushion the blow to the reputation of the financial institution targeted by the attack is to ensure that, no matter what, the customers gets his money back, and does so swiftly.

From a technical point of view, there are special procedures in place for when an attack occurs: there are international and local bodies to zero in on the nature of the fraud, determine who's in charge given the situation and who is to ultimately refund the customer's money. There are, of course, simple rules in place for this: in the case of a skimmed card – simply an illegal, forged copy of the original — the bank is liable as per the card issuers governance. But, if the card has been misplaced or physically stolen, then the customer is ultimately responsible.

The biggest issue in the UAE, however, is ATM and POS-terminal fraud – those comprise the primary features of this market; online fraud is not as prevalent here as it is in other parts of the region. To combat this type of card-based fraud, banks need to be equipped with sophisticated tracking tools for every device (skimming is very popular). To further curb this threat, it is better to lower the limit of withdrawal, or even better to use special rules and filters which will not influence the customers, but will be able to backtrack and retrieve the entire picture, should the card be stolen. This will also make it easier to save the customer's money, as well as the bank's reputation.

But response really is the last step; the best way to protect a bank's reputation is to not allow any fraudulent attacks on its customers. I would suggest being very precise in selecting the best prevention solution.

At BPC Banking Technologies, we offer a sophisticated system to prevent fraud. Our advanced fraud prevention solutions help card issuers and acquirers combat the growing threat of card-based fraud by monitoring a hundred percent of all transactions, online, in real-time, across all channels. The solution's powerful and flexible rules-based engine ensures that its users can rapidly implement their monitoring policies, and rest assured in the knowledge that they can prevent fraud before unauthorised transactions are processed, and before their customers or their businesses are affected in the slightest.

BPC' SmartGuard solution, part of the SmartVista suite – a single integrated solution for transaction processing and card management – matches transactions against a set of business-driven rules, suspicious transactions are rapidly detected and stopped. FME