

NCR PERSPECTIVE

Innovation and collaboration undermine global ATM crime

Today the three major threats are card skimming, explosive attacks and cyber crime

Card skimming still represents the biggest cost to the industry in terms of hard cash losses

By Paul Race, Vice President of Marketing Services, NCR

Despite the emergence of chip and PIN technology and a range of risk mitigation solutions, criminals continue to seek out any weak link in the chain of ATM defence. ATM deployers are winning individual battles, but the war against ATM crime is ongoing and the means of engagement continually shift as new challenges emerge.

Today the three major threats are card skimming, explosive attacks and cyber crime. EAST (European ATM Security Team) has also reported a recent increase in cash trapping on certain ATM model types. Since the rewards of this type of fraud are limited, this trend may reflect a migration away from card fraud due to the success of EMV and other methods of combating skimming.

In order to counter the evolving nature of ATM crime, a multi-faceted response that includes innovation, collaboration, people, technology and processes is required. As an industry we can remain proactive and vigilant in undermining criminal activity with this approach.

Skimming attacks – gaps in the defence

Card skimming has a long history and still represents the biggest cost to the industry in terms of hard cash losses. Despite the introduction of EMV (with 97% of all European ATMs now compliant) the continued existence of the magnetic stripe on cards provides an opportunity for skimming. However, the good news is that though criminals remain persistent and card skimming attacks at the ATM have increased by 3%, during 2010 losses have fallen by 14% (EAST).

This is only the European side of the story. Fraud always migrates to the weakest, unprotected areas. A delay in the introduction of EMV technology in the USA has left the market exposed where conservative estimates put card skimming losses at around \$1 billion. Furthermore, card data captured

in the UK, for instance, can be used to withdraw funds in countries without chip and PIN technology, such as the USA.

However, significant moves are now being made towards closing this loop. News that Visa and MasterCard are introducing a liability shift for EMV compliance in the USA means that we can hope to see the decline of the magnetic stripe. Meanwhile, a report from the European Central Bank / Eurosystem recommended that all new SEPA (Single Euro Payment Area) cards should by default be 'chip only' cards from 2012 onwards. If the industry, for practical reasons, opts to retain the magnetic stripe, the other recommendation was that it should not contain payments data. It does, however allow for the issue of legacy magnetic stripe cards, for example where a customer wishes to travel outside Europe to countries that have not yet implemented chip technology.

Physical attacks – explosive development

An examination of physical attacks on ATMs provides mixed messages. In Europe, the number of incidents reported by EAST in their 2010 report has declined, but the amount stolen has increased by 18%.

What is noticeable is the determined nature of these attacks, with an 88% increase in explosive attacks, including gas as well as solid explosives.

Digital crime and data breaches – internal and external threats

Viruses used to be perceived as the main software hazard, however, there is now widespread recognition of the very real threat from digital crime. This is highlighted by ATMIA's 2011 *Global ATM Crime Survey*, in which cyber attacks were ranked third out of all ATM threats. As well as an increase in malware attacks specifically designed to undermine a system and exploit its weaknesses (reported in Verizon's 2011 *Data Breach Investigations Report*), there have also been high

profile insider attacks. Bank employees have used their knowledge of the banks' software systems to steal data and commit fraud that has amounted to millions of dollars. Data breaches have also been linked to incidences of card skimming, where stolen data has been used on cloned cards. All this highlights the need for increased data security.

A wide-ranging response to a complex problem

The payment card industry has introduced a security ecosystem to limit the risk of fraud. PCI-DSS includes security management, policies and procedures, network architecture and software design. For ATM deployers, investment in achieving and maintaining compliance not only reaps rewards in terms of improved security but is also dwarfed by the costs of not complying, particularly when it comes to a fraudulent incident damaging a bank's reputation.

The *2011 Data Breach Investigations Report* confirmed that of those institutions that suffered a data breach in the previous year, 90% were not PCI-DSS compliant.

Complementary countermeasures ensure that with collaboration between deployers and law enforcement agencies, criminal activity will be successfully undermined going forward. These include best practices of anti-skimming approaches and the proactive use of cameras with analysis and detection systems.

Awareness and early response

Since fraud is a global problem and criminal modus operandi migrate quickly, communication regarding ATM attacks and fraud is essential in enabling deployers to respond to the latest trends and to stay ahead of criminals. The emergence of new, smaller card skimming devices and the placement of pinhole cameras are examples of the need to keep branch staff informed and vigilant in spotting potential devices.

At NCR we are keen to collaborate further in raising awareness about new ATM crime incidents, and would welcome notifications of new attacks via Global.Security@ncr.com.

Innovative security measures

As part of its holistic approach to security, NCR continues to work with customers to develop new innovative fraud prevention measures. One

such solution has been introduced by a northern European deployer that has invested heavily in EMV technology. The solution provides two card readers, one for cardholders who only have a magnetic stripe card and a second 'half-dip' card reader for cardholders with a chip-enabled card. The latter reads the chip but does not fully read the magnetic stripe. Criminals attempting to obtain information via the use of a skimming device will be prevented from copying the data from the magnetic stripe. As well as reducing losses, the other benefit to the bank of marketing this enhancement has been a significant increase in the number of 'on-us' transactions.

Design against crime

As part of its comprehensive campaign to reduce the threat of ATM fraud, NCR has worked closely with research organisations in the UK, the Netherlands and Australia to explore innovative design features that may deter criminal activity.

For example, amongst the designs from Central Saint Martin's College of Art and Design in London is a 'magic carpet'. It helps control the space directly behind and to the side of a person entering the PIN at an ATM and is an effective means of discouraging 'over the shoulder' surfing of PIN numbers. One of its features is the sounding of an alarm if another individual, deliberately or inadvertently, invades the ATM user's space.

Bob Tramontano, vice president of financial industry marketing at NCR, said, *"The fight against ATM crime is ongoing. It involves innovation, collaboration with law enforcement agencies and deployers, the provision of best practice advice to clients and via them to consumers, as well as the development of new technologies and processes that make the ATM more secure and at the same time support the industry requirement for PCI compliance.*

NCR continues to champion the need for a multi-faceted industry response to fraud. While there is evidence of true progress – European losses from fraud attacks have fallen 28% from €144 million to €112 million – criminals do not stand still and there remains much work to be done to stay ahead of the constantly evolving threats." ■

For more information on security solutions and best practice please contact us at: NCRSelf-Service.Security@ncr.com

Of those institutions that suffered a data breach in the previous year, 90% were not PCI-DSS compliant

Communication regarding ATM attacks and fraud is essential in enabling deployers to respond to the latest trends

