

DIEBOLD PERSPECTIVE

ATM crime:

An ever-evolving global threat

Meet the security challenge with a multi-layered approach.



Aleksandra Lubavs
Diebold EMEA

By Aleksandra Lubavs, Director, Marketing, Communications & Strategy, Diebold EMEA

From the day automated teller machines (ATMs) first appeared, financial institutions have made it a priority to secure them. In the more than 40 years since the ATM was introduced, criminals have become increasingly sophisticated. They strive to breach the machines, trying to access either the cash inside or the account information of the consumers who rely on the devices for their banking needs.

Today, criminals perpetrate ATM crime in a variety of ways. Physical assaults, such as ramming terminals or attempting to remove them from their locations, are the most brazen. Less violent, but more threatening, is the installation of malware to infiltrate the ATM's internal data network and enable the theft of account information. Skimming and trapping methods steal magnetic-stripe data and personal identification numbers (PINs) while unknowing customers are completing transactions.

In Europe, the European ATM Security Team (EAST) reported that ATM-related fraud losses totalled €312 million for 2009. Between 2008 and 2009, ATM attacks rose 8%, from 12,278 fraud incidents to 13,269, in the 32 countries that are a

part of the organisation. Clearly, ATMs remain very much under threat globally.

To anticipate and mitigate ever-evolving threats to the self-service channel, financial institutions must be vigilant in their efforts to protect ATMs from a variety of attacks, from the most basic physical violations to the most sophisticated network schemes.

Understand the security landscape

Even as new innovations in ATM security are developed, the threat continues to evolve. The most current information and tools to help criminals breach ATMs are readily available via the Internet. Thieves are increasingly organised and able to commit crimes rapidly around the world. It is becoming more difficult to apprehend them.

Some skimming devices, for example, are so advanced that they employ Bluetooth technology to enable the wireless transmission of stolen card data and PIN information. The use of such technology means thieves no longer need to return to the ATM to retrieve the skimming device and stolen information, thus decreasing their risk of detection.

At the same time, financial institutions, in growing numbers, are changing the service model within their branches, driving basic transactions – such as withdrawals and deposits – out of the teller line and assigning them to the ATM. With the ATM channel becoming even more pervasive, the assets and brand reputations of financial institutions are more dependent than ever on effective ATM security solutions.

Take a multi-layered approach

Creating and executing an effective strategy for ATM security is among the biggest challenges facing financial institutions today. Meeting the challenge requires the implementation of a comprehensive, multi-layered approach to security that includes hardware, software and services. Financial



institutions can gain valuable assistance by forming a strategic alliance with a proven security provider.

A third-party expert can help develop a strategy that proactively looks at the self-service experience from a broad security perspective. This comprehensive view encompasses physical and logical security, as well as fraud detection. The multi-layered approach includes assessing risk for each terminal based on location and environment while also educating consumers about good security practices.

Fight back against skimming

The multi-layered approach of combating ATM crime extends to specific defences against skimming, considered by financial institutions around the world to be today's greatest threat to ATM security.

First identified in Europe, skimming is a crime of low risk and high reward, typically requiring only the attachment and later detachment of skimming devices to ATMs in order to obtain consumer card data and PINs. It is a threat not just to ATMs, but to all self-service technology, from point-of-sale devices to self-service fuel pumps in petrol stations to check-in kiosks at airports.

Financial institutions must implement anti-skimming solutions that offer multiple layers of protection. The protection should range from basic solutions

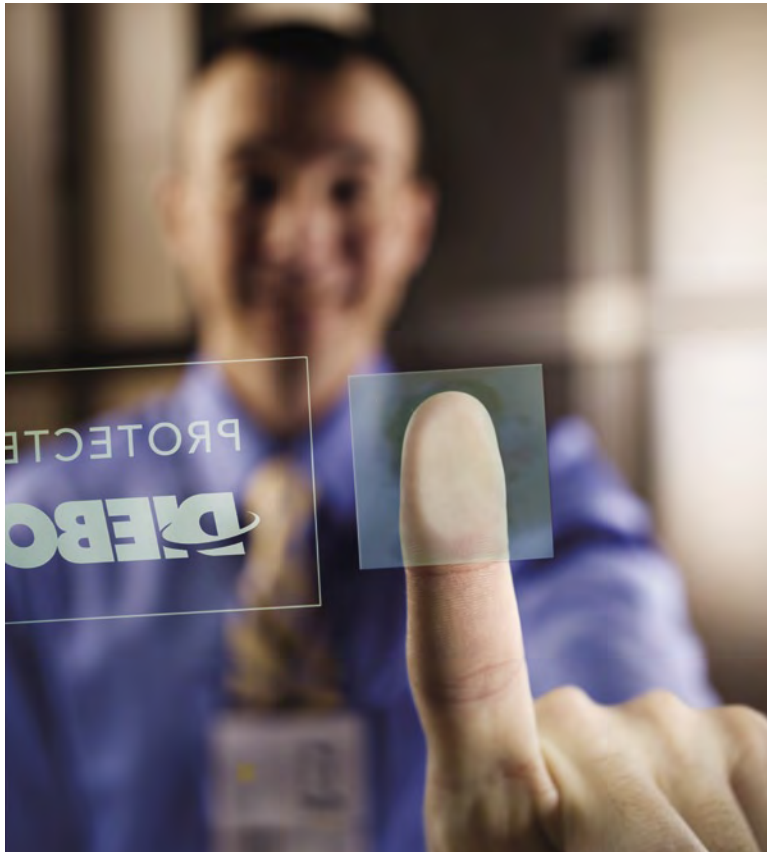
for card-reader security to higher levels of fraud mitigation, such as skimming detection alerts and real-time ATM security monitoring.

Create a customised solution

Financial institutions can help mitigate ATM crime by investing in a strategic alliance with an expert that can develop security solutions customised to their needs. Believing security is at the core of any ATM network, Diebold is a proven resource in developing industry-leading solutions to physically protect the ATM, safeguard the data assets of the ATM and its users, and secure the entire ATM environment. Diebold combines more than 150 years of industry thought leadership in the field of security with financial self-service expertise, to ensure it understands the very latest security risks facing financial institutions and to deliver maximum protection for assets and customers. Diebold's global ATM Security team is helping to fight evolving threats to ATM integrity by delivering customised and seamlessly integrated multi-layered security solutions. ■

For more information, including a white paper offering a closer look at a multi-layered approach to ATM security, please visit: www.diebold.com/atmsecurity/security.

Thieves are increasingly organised and able to commit crimes rapidly around the world. It is becoming more difficult to apprehend them



DIEBOLD
INNOVATION DELIVERED®