

WINCOR NIXDORF PERSPECTIVE

Creating a protective shield for banks

By Uwe Krause
Director Global Marketing, Wincor Nixdorf



Uwe Krause
Wincor Nixdorf

Criminals are at work wherever money changes hands – branches are attacked, networks are hacked and ATMs are manipulated. According to the FBI, attacks on bank branches resulted in losses of over \$43 million in the USA in 2010, and the European ATM Security Team (EAST) reported that in Europe, nearly €33 million was lost in ATM related physical attacks such as ram raids, ATM burglaries and robberies.

The methods used by criminals to steal cash or attack systems for handling electronic payment transactions are becoming increasingly sophisticated. Banks require physical protection, such as security for hardware and buildings, but also logical protection for the security of networks and software. This has driven a demand for end-to-end security solutions that prevent attacks on processes and delivery channels.

ATMs a prime target

More than 12,000 fraud attacks against European ATMs were reported last year. Card skimming accounted for 85% of these cases, but techniques

such as card trapping, cash trapping and transaction reversal fraud brought total losses to over €268 million, according to EAST. The number of attacks on ATMs has been rising, along with an increase in the variety of manipulation methods.

Banks are fighting back, improving the security of self-service transactions by equipping ATMs with cameras in order to visually document cash withdrawals from start to finish, and to deter criminals from tampering with machines. Using optical surveillance technology is an effective way of preventing attacks on ATMs.

Another valuable means of ensuring greater security is the use of remote surveillance solutions. Through continuous remote monitoring of all ATM systems, such solutions can access important information – for example, details of attempts to tamper with ATMs – which can be used to evaluate incidents and formulate appropriate responses.

The protection of self-service systems is a key focus of banks, and there is a demand for security solutions that defend against high-tech thieves and counteract the growing number of manipulation attempts at ATMs.

Payment card fraud remains a challenge

Hacking, phishing and other abuses of payment card data are major challenges for deployers of electronic payment systems. The UK Cards Association estimates that in the UK alone total fraud losses on cards were worth £365 million in 2010, with online banking fraud totalling £47 million.

Fraudsters are networked globally, highly creative and quick to pounce. What is needed is a comprehensive solution that links information from several payment transaction systems and channels (e.g. POS devices, ATMs), and provides protection for both customer accounts and terminal systems. The solution must be integrated into the authorisation process in real time, and take into account location and behaviour patterns.



Furthermore, it must detect new fraud trends with minimal data so that it can react immediately.

ProTect ATMs with anti-skimming and monitoring solutions

Wincor Nixdorf's *ProTect* offers physical security as well as logical protection for software and networks, and acts as a protective shield for electronic payment transactions. The company's portfolio of security products has been specifically designed to address the issues currently challenging banks, and provides an end-to-end security solution.

The new *Anti-Skimming II* module thwarts attempts to steal card data at ATMs. It detects skimming devices, triggers a silent alarm and initiates other actions such as video monitoring. It also emits an interference field that prevents sensitive card data from being read. The advantage of this technology is that it simultaneously prevents skimming attacks while allowing business to continue uninterrupted for customers.

Optical Security Guard is Wincor Nixdorf's system monitoring solution. It protects the new CINEO systems from a wide array of attacks. The use of intelligent recognition processes means that criminal alterations to ATMs, such as keypad overlays, skimming devices, hidden or disguised cameras, or other changes (such as those that enable cash trapping) are identified immediately.

Finally, Wincor Nixdorf's *ProView* is a solution for the monitoring and control of self-service networks. It is evolving into an IT management platform: ATMs, transaction terminals and POS systems in retail environments can all deliver information beyond their operating status. New-generation CINEO systems, for instance, can supply detailed information on the cash holdings in every device – data that can be used to optimise cash cycle management. *ProView* can also provide background systems with critical information, such as notification of attempts at ATM tampering. *ProView* is already in use on multivendor systems in 65 countries on five continents. It is also supported by *ProView Video Surveillance*, software that enables centralised image and video monitoring and image analysis.

Securing payment card systems with ePayment Solutions – Fraud Prevention

Wincor Nixdorf's *ePayment Solutions – Fraud Prevention* is a state-of-the-art, highly flexible solution for detecting cases of payment card fraud.



It follows a multichannel strategy, combining and evaluating information from any payment channel. Data from card transactions, online banking or mobile banking can be linked and analysed in real time. Highly suspicious transactions can be rejected during the authorisation process with a hitherto unmatched accuracy. *ePayment Solutions – Fraud Prevention* reacts to unusual behavior – for example, attempting to access an account online from a new IP address to transfer money to a suspicious target account, followed by attempts to withdraw large sums of cash from an ATM shortly afterwards. It is a highly flexible, proactive tool for revealing complex interrelationships as quickly as possible.

With *ePayment Solutions – Fraud Prevention*, Wincor Nixdorf also extends a protective shield to other payment channels. Its goal is to reduce all fraud-related costs and increase customer satisfaction. Whenever there is reason to suspect that customer data has been compromised, the respective cards and accounts can be kept under surveillance. The cards in question need only be replaced in the case of an actual fraud attack. As a result, negative publicity and the cost of card replacement are avoided.

With its end-to-end concept *ProTect*, Wincor Nixdorf offers a coordinated strategy for greater security in payment transactions and effective protection at ATMs and terminals for bank cardholders.

The company's extensive portfolio of security solutions is rounded out by consulting and other services. Based on a detailed analysis of an ATM operator's existing security processes, Wincor Nixdorf's experts can develop tailored solutions that can range from individual projects to the complete monitoring of all systems and bank branches. ■



**WINCOR
NIXDORF**