WHITE PAPER

atm marketplace

ATM Fraud Prevention

With criminal syndicates increasingly targeting ATMs, the need for greater data security has become more apparent than ever.

SPONSORED BY:

National Cash systems

By Robin Arnfield
ATMmarketplace.com

As other countries have migrated to the EMV (Europay, MasterCard and Visa) card security standard, the U.S. has become increasingly vulnerable to card fraud at ATMs and POS terminals. The European ATM Security Team has said that the U.S. is now the top destination for ATM fraud attacks such as magnetic-stripe card skimming, which has migrated from European EMV-compliant countries.

Card analytics firm FICO said that data from its FICO Card Alert Service revealed a 48 percent increase in U.S. ATM fraud as a result of skimming between 2012 and 2013. And the cost per incident has risen significantly. "According to a report from the U.S. Secret Service, the cost of an ATM skimming incident in the U.S. has risen to $50,000 on average, up from $30,000 a few years ago," retail ATM vendor Triton Systems said in a blog post.

In addition to skimming attacks, ATMs are vulnerable to hackers and to malware that is placed on the machine locally — for example, through USB devices — or via unsecured network connections.

Protecting customer data

In its "Best Practices for Merchant Account Data Security" blog, Irvine, California-based ATM solutions provider National Cash Systems said merchants need to be highly aware of the risk of malicious acts of data hacking and realize that, if customers' account data is left unsecured, it can result in major losses for their business.

National Cash Systems stressed that the merchant is responsible for protecting customers' PIN and card data encoded on a magnetic stripe or EMV chip — e.g., primary account number (PAN), cardholder name, expiration date and card-verification code or value — for both ATM and point-of-sale transactions.

PCI DSS

ATM operators must comply with the Payment Card Industry Security Standards Council standards, the most important of which is the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS includes requirements for password management, network security and the implementation of system access controls. Its purpose is to protect cardholder information from unauthorized access by setting enforceable standards for the quality of an organization's information security practices. Penalties for noncompliance with PCI DSS include substantial fines from the card schemes, as well as liability for fraud losses resulting from data breaches.

Each area of an ATM that processes cardholder data has to meet PCI DSS requirement 3 — "protect stored cardholder data" — which says that the full contents of a mag-stripe track or EMV chip and PIN (also referred to as "full track" data) must not be stored by a payment system.

The only cardholder data that may be stored after authorization is the PAN, expiration date, cardholder name and service code. Cryptographic keys should be used to protect stored data, and PANs should be rendered unreadable through the use of truncation, PCI DSS stipulates.

Passwords

Effective password controls are essential for ATM security. "It's a very bad security practice to have the same admin password for all your ATMs," said Steve Hensley, executive vice president of global sales at KAL ATM Software.

As hackers might know vendor-supplied default system passwords, PCI DSS requires that ATM operators select new passwords when commissioning new ATMs.

Anti-skimming protection

ATM operators should deploy physical security measures such as an anti-skimming device.

There are two types of skimming attack. "In a digital skimming attack, criminals place a device on an ATM which looks like a card reader and copies the data when the card is passed through the device," Triton said in a blog post. "The data is stored in the skimmer's memory and is downloaded to a PC where it can be read and used to make fake cards. In an analog skimming attack, criminals record the sound of the card's data signal during the transaction. The data is retrieved from the recording and used for fraudulent purposes."

Triton quoted Douglas Russell, director of DFR Risk Management, as saying that anti-skimming devices have been extremely successful in using electromagnetic signals to distort card data.

> **"You should run software that can tell if an ATM has been tampered with — for example, by a skimmer being attached — and sends an alert with the option of shutting down the ATM."**
>
> *— Steve Hensley, executive vice president of global sales at KAL ATM Software*

Vendors such as Wincor Nixdorf and NCR have developed technology that prevents both types of skimming.

ACG has developed the Enhanced Card Security (ECS) anti-skimming device, which is compatible with NCR, Wincor Nixdorf, Diebold and Nautilus Hyosung ATMs. ECS deactivates skimming devices by generating distorting frequencies as cards pass through the ATM card reader. According to ACG, ECS incorporates anti-card-trap technology and provides a data-logging facility, enabling the device's status data to be monitored remotely.

Update software

ATM deployers must keep the application software and operating system running on their ATMs up to date to ensure that they have the latest security patches. It's also essential that ATM operators keep their antivirus software and other security programs such as firewalls updated.

Hackers thrive on old software because they can exploit its weaknesses, according to "Securing ATMs with Software: Five Strategies," an ATM Marketplace white paper sponsored by Triton.

ATM vendors provide regular application and operating system software upgrades, which are easy for ATM deployers to install, Triton said.

Windows XP

On April 8, 2014, Microsoft ceased to provide updates for Windows XP, although it will continue to supply its Malicious Software Removal Tool to XP users until July 14, 2015.

This means that ATMs that haven't migrated from Windows XP to Windows 7 won't receive Microsoft security patches. They will face greater risks from malware and network intrusions and will be in breach of the PCI DSS requirement for ATM deployers to keep their operating systems updated with security patches protecting against known vulnerabilities.

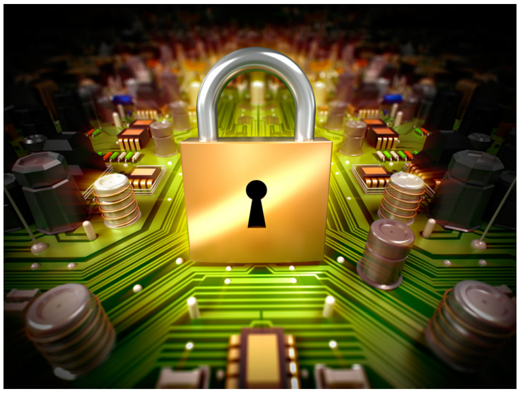
ATM deployers who face delays in migrating their ATMs from Windows XP to Windows 7 have two options. First, Microsoft will provide an extended custom technical support contract — a Custom Support Agreement — to organizations still running XP. The cost of this support is so high that it is more cost-effective for most ATM deployers to migrate to Windows 7 than to pay Microsoft for security patches for their XP-based ATMs.

Second, several ATM vendors offer security technologies to mitigate the risks faced by ATM deployers who haven't completed their Windows 7 migration. For example, NCR offers the Solidcore Suite for APTRA, while Wincor

Nixdorf provides the PC/E Terminal Security system for XP-based ATMs. These technologies employ whitelisting security software, which allows only explicitly identified software to run on ATMs. Any malicious software, including attacks that exploit new vulnerabilities in XP, is prevented from running.

The PCI SSC has said that if ATM deployers run "compensating controls" — i.e., whitelisting security software, active monitoring of system logs and network traffic and isolating XP-based ATMs from the Internet — until migrating to Windows 7, they might be able to comply with PCI DSS requirements. However, those compensating controls should be seen as a temporary measure, and an active Windows 7 migration plan should be in place.

Also, if an ATM running XP is Internet-facing, it will be detected and reported as an automatic failure in a PCI DSS compliance scan by an approved scanning vendor, the PCI SSC has warned.



Lockdown

The ATM Marketplace report "EMV, PCI and the ATM Industry" said that ATM deployers need to lock down their machines so that unused hardware or network ports are disabled and can't be used by hackers or malware. This action involves allowing only features that are necessary for the operation of the ATM and disabling extraneous features, as well as making all electronic points of entry invisible to hackers and malware.

ATM deployers also should use security technology such as Wincor Nixdorf's PC/E solution, which locks down ATM operating system software by disabling or removing extraneous components and services and reducing the "attack surface."

If criminals are able to compromise an ATM's operating system, they can gain access to all the data that passes through the ATM's operating system and memory.

"It's vital for ATM deployers to lock down their ATM software, so that it cannot be hacked into or changed," Hensley said. "ATM fraud can occur because people have access to the hardware and install a keyboard or a USB drive or insert a DVD into the DVD reader."

Collaboration

"ATM fraud prevention has to be a collaboration between ATM operators, ATM manufacturers, ATM servicers and consumers," said Jim Outland, president of U.S. consultancy Paragon Data Services. "ATM operators must make fraud detection and prevention a top priority, which can be greatly enhanced by implementing the fraud- and tampering-detection tools available from ATM manufacturers, redoubling ATM inspections for tampering when the ATM is serviced and educating consumers about fraud detection and prevention."

Outland said that consumers play a pivotal role in fraud detection and prevention by being aware of their surroundings at ATMs and alert for changes or abnormalities in the ATM keyboard, card reader or operation.

> **"The best ATM security practice is to get regular software updates, operate effective password management and lock down your ATM software so it can't be hacked or changed."**
>
> *— Steve Hensley, executive vice president of global sales at KAL ATM Software*

About the sponsor:

Since 1997, National Cash Systems has established many successful relationships with thousands of merchants nationwide. The company's successful track record in providing clients with turnkey ATM and comprehensive payment solutions has earned it a reputation for delivering quality products while exhibiting financial stability and expertise. For more information, visit www.nationalcash.com.

Five key areas to address:

1. **Consult software and hardware vendors.**
   To ensure the safety of consumer data, determine with the software vendor whether the ATM or POS terminal operating system stores sensitive information from a payment card magnetic stripe. Talk to hardware and software vendors or ATM merchant services providers about various ways to ensure data security.
2. **Take additional protection measures.**
   Ensuring the full security of POS terminals and ATMs means that operators won't let customers down, and it gives them the opportunity to win a reputation as a trustworthy merchant. Simple practices such as hashing, truncation and data encryption can reduce risk considerably. It is advantageous to find out from credible sources about consumer data that can be stored legally and securely.
3. **Limit access to sensitive information.**
   A good way to ensure data security is to practice vigilance on all communications channels, including telephone conversations, and allowing access to sensitive information only after authentication.
4. **Ensure system security.**
   Protecting data and business information with firewalls, antivirus programs, encryption and other security software will prevent criminals from gaining access to the computer system. Stay ahead of the hackers by keeping up to date with data security best practices.
5. **Adopt security policies.**
   Formulate a data security policy for the business and share this information with all employees. Outline all security programs and procedures that everyone must comply with. Companies that offer custom ATM programs and merchant services specialize in providing secured ATM and card processing solutions. Operators also should refer to the PCI DSS to formulate their security policy

Source: National Cash Systems (http://www.nationalcash.com/blog/)