ATM Fraud and Security 101

By Robin Arnfield | Contributing writer, ATM Marketplace

atm marketplace

CONTENTS

Published by Networld Media Group © 2015 Networld Media Group
Written by Robin Arnfield, contributing writer, ATMmarketplace.com
Tom Harper, president and CEO
Kathy Doyle, executive vice president and publisher
Suzanne Cluckey, editor
Brittany Warren, custom content editor

EXECUTIVE SUMMARY

By Robin Arnfield | Contributing writer, ATM Marketplace

This report explains key ATM fraud and security risks such as skimming, physical attack, malware and cyberattack. It also provides guidance on ATM security best practices and industry requirements, such as EMV and PCI DSS.

As the U.S. payments industry prepares to migrate to EMV chip technology, the nation's ATMs have experienced a surge in skimming attacks. In addition, ATM fraud has migrated to the U.S. from Europe, which has already completed its EMV migration.

The European ATM Security Team says that the U.S. is second only to Indonesia number of ATM fraud attacks such as mag stripe skimming, which has migrated from European EMV-compliant countries.

Once it has migrated to EMV, the United States can expect a rise in ATM malware and cyberattack, as well as physical attacks such as smash-and-grab raids and explosive gas attacks.

ATM deployers who suffer a security breach will face not only damage to their reputation and loss of business, but also fines from the card networks and, potentially, lawsuits from issuers for any fraud losses that result from a data breach.

"Securing ATMs and POS devices isn't just about preventing monetary losses — it's also about protecting something far more valuable, which is your customer's trust," Wincor Nixdorf Senior Trusted Advisor Terence Devereux told ATM Marketplace.

Robin Arnfield has been a technology journalist since 1983. His work has been published in ATM Marketplace, Mobile Payments Today, ATM & Debit News, ISO & Agent, CardLine, Bank Technology News, Cards International and Electronic Payments International. He has covered the United Kingdom, European, NorthAmerican and Latin American payments markets.

© 2015 Networld Media Group

CHAPTER 1

Introduction

The U.S. is experiencing a surge in ATM fraud before the country migrates to EMV.

MasterCard and Visa have established deadlines for shifts in counterfeit card fraud liability for U.S. acquirers who don't upgrade their ATMs and POS terminals to meet EMV specifications.

The deadline for merchant POS terminal EMV migration is October 2015; MasterCard and Visa have set October 2016 and October 2017, respectively, as deadlines for U.S. ATMs. (In addition, U.S. fuel dispensers face an October 2017 EMV migration deadline.)

After these deadlines, if an EMV card is used fraudulently at an ATM that doesn't support EMV, the acquirer will be liable for the issuer's fraud losses. ATM deployers who do not migrate to EMV risk being shut out of their acquirer's network.

Lack of EMV readiness

According to an August 2015 atmAToM.com blog by Darryl Cornell, president and CEO of Long Beach, Mississippi-based ATM vendor Triton Systems, many U.S. merchants aren't upgrading to EMV, despite the fact that processors are mostly ready.

"A July 2015 Wells Fargo/Gallup Small Business Index survey found that only 49 percent of small merchants (under $20 million) are even aware of [the October 2015] EMV POS liability shift deadline," Cornell wrote.

"Nearly 70 percent of merchants aren't ready [for EMV], and over half of those unprepared merchants will either be late to the EMV party or have no intentions of upgrading their POS terminals. Presumably, these same merchants are also not in a hurry to upgrade their ATMs or fuel pumps. Given that accumulated chargebacks can take as long as 90-days to work their way through the system, look for the first howls of merchant liability shift pain in December 2015."

According to Cornell, vendors are reporting that nearly all new ATMs sold in the U.S. in 2015 have been equipped with EMV card readers.

© 2015 Networld Media Group

“Most banks are moving forward with their EMV upgrade programs, which in many cases were accomplished along with Windows 7 upgrades,” Cornell wrote. “However, anecdotal reports indicate that fewer than 10 percent of retail ATMs are currently EMV-ready. While there has been movement on the part of larger IADs to begin purchasing upgrade kits and replacement units, most IADs plan to wait until 2016 to begin upgrading their own terminals.

“Even if this does happen, convincing merchants to upgrade or replace their owned ATMs will likely prove to be heavy sledding. Look for a serious contraction in retail ATMs beginning in late 2016 as sponsor banks, processors and IADs pull the plug on non-EMV terminals rather than chasing merchants for fraud losses.”

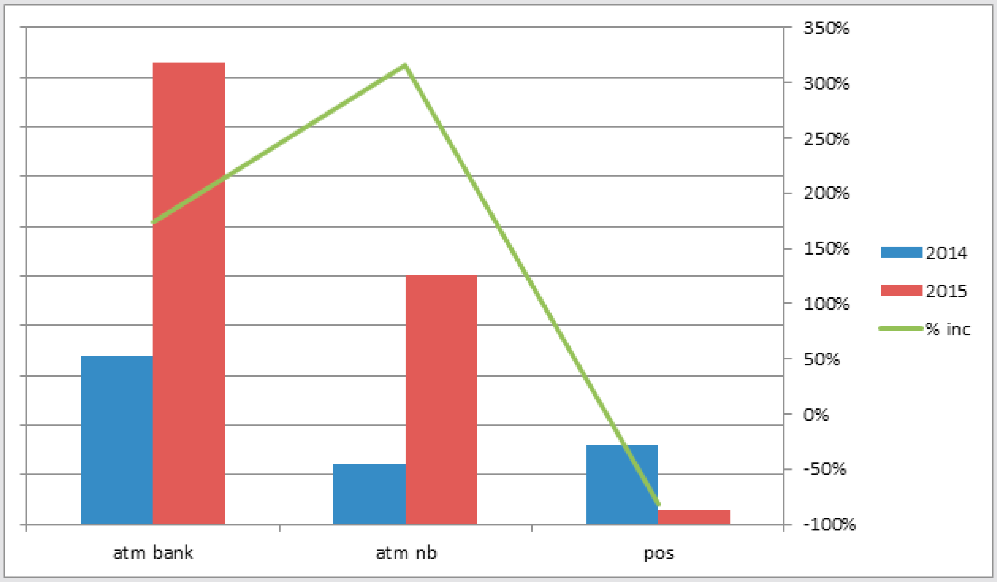
U.S. fraud data

In May 2015, U.S.-based credit scoring and fraud analytics software firm FICO warned that cardholder data theft at U.S. ATMs had reached its highest peak in over 20 years.

According to FICO, between Jan. 1 and April 9, 2015, debit card data theft rose by 174 percent at U.S. bank-owned ATMs compared year-over-year and by 317 percent at nonbank ATMs. However, during the same period, card data theft at POS terminals in merchant locations dramatically declined by 81 percent, FICO said.

“We’re seeing a lot of fraud in the U.S. as criminals try to exploit the lack of EMV protection before it is implemented in the U.S., and before the liability shift at the point of sale takes effect,” said Martin Warwick, FICO fraud chief in Europe, the Middle East and Africa. “Having EMV will make the mag stripe data less appealing to criminals.”

Card and PIN Points of Compromise Cases Identified by FICO Card Alert Service



Source: 2015 FICO® Card Alert Service

> **“We are seeing a lot of fraud in the U.S. as criminals try to exploit the lack of EMV protection before it is implemented in the U.S. Having EMV will make the mag stripe data less appealing to criminals.”**
>
> Source: Martin Warwick, FICO fraud chief for Europe, the Middle East and Africa.

Canada

Triton’s Cornell wrote in an ATM Marketplace blog that Canada saw positive results from its migration to EMV.

Citing statistics from Interac, Canada’s domestic debit card scheme, Cornell wrote that Canadian domestic debit fraud at ATMs averaged nearly CA$2,400 ($1,822) per terminal in 2009.

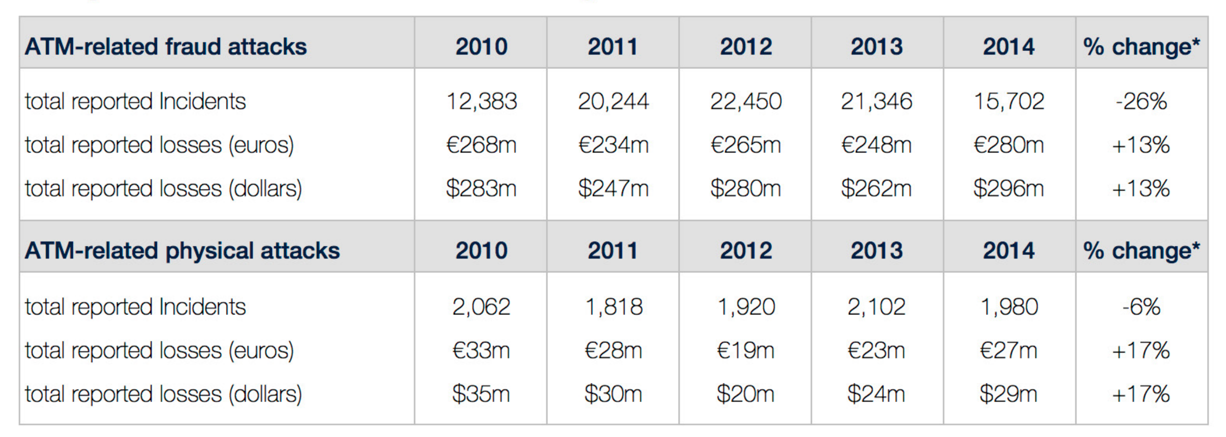
“By 2014, two years after Canada’s migration to EMV, that figure had been slashed to a mere CA$33 ($25) per terminal,” he wrote. “An interesting aside is that all non-EMV ATMs were turned off by Interac in December 2012 — a reduction of nearly 1,000 terminals.”

Europe

In July 2015, the European ATM Security Team published the second of three European fraud updates for 2015. The report was based on ATM crime statistics gathered in June 2015 from 19 countries in the Single Euro Payments Area (SEPA), and from two non-SEPA European countries.

Card skimming at ATMs was reported by 17 countries, with decreases reported by seven countries and increases by two, EAST said. Six countries reported card data compromise through

European ATM crime statistics summary



ATM-related fraud attacks	2010	2011	2012	2013	2014	% change*
total reported Incidents	12,383	20,244	22,450	21,346	15,702	-26%
total reported losses (euros)	€268m	€234m	€265m	€248m	€280m	+13%
total reported losses (dollars)	$283m	$247m	$280m	$262m	$296m	+13%
ATM-related physical attacks	**2010**	**2011**	**2012**	**2013**	**2014**	**% change***
total reported Incidents	2,062	1,818	1,920	2,102	1,980	-6%
total reported losses (euros)	€33m	€28m	€19m	€23m	€27m	+17%
total reported losses (dollars)	$35m	$30m	$20m	$24m	$29m	+17%

Source: EAST European ATM Crime Report 2014

**2013-2014*

© 2015 Networld Media Group

wiretapping or “eavesdropping,” in which criminals cut a hole in the fascia by the card reader, insert a device that is then connected to the card reader, and cover the hole with a fake decal.

In its July report, EAST said that the trend of skimming-related losses occurring outside of EMV chip liability shift areas continues. These losses were reported in 49 countries and territories outside SEPA and in 10 within SEPA. For the first time, Indonesia was the top location for such losses, displacing the U.S. The Philippines ranked third.

Fourteen countries reported cash-trapping attacks, and seven reported incidents of transaction reversal fraud, which involves an error condition being created at the ATM, which makes it appear that cash won’t be dispensed, EAST says. This forces a re-credit of the amount withdrawn back to the account when, in fact, the criminal gets the cash through the insertion of a device or by manual manipulation of the ATM dispensing mechanism.

Four countries reported ATM malware incidents, which involved ATM cash-out or “jackpotting” (see Chapter 2 Malware, page ?). In two countries, these were first-time occurrences.

Nine countries reported Ram raids and ATM burglary. Eleven countries reported explosive gas attacks; two also reported attacks on ATMs using solid explosives.

The U.K.

In 2014, the percentage of fraudulent transactions occurring outside of the U.K. on debit cards issued within the U.K. rose by 25 percent, according to a FICO study cited by ATM Marketplace.

In a study of 52 million active U.K. debit cards, FICO said it found that fraudulent cross-border transactions accounted for nearly one-third (31 percent) of all fraudulent transactions in 2014, compared with 23 percent in 2013.

Citing an “unprecedented spike in fraudulent U.S. ATM cash-outs,” FICO said the U.S. accounted for 47 percent of all fraudulent cross-border transactions on U.K. debit cards in 2014. But while it ranked first for the number of fraudulent cross-border transactions on U.K. cards, the U.S. ranked only third for cross-border transactions on U.K. cards overall.

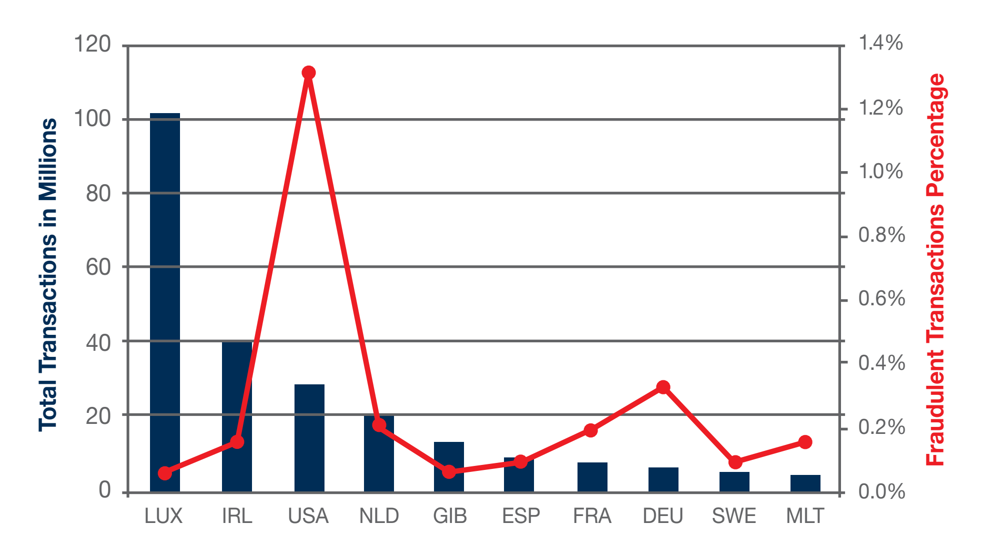
While 24 percent of debit card transactions occurred at ATMs, 12 percent of fraudulent transactions came from ATMs, FICO found. Still, ATMs topped the list of merchant categories for fraudulent debit card use.

FICO’s Warwick said that an “alarming” rise in cross-border fraud demands new technology, such as proximity location services that can identify whether the customer’s mobile phone is in the same place as the transaction in progress.

The cards in FICO’s sample represented 5.6 billion total transactions worth 306 billion pounds ($474 billion), a 5 percent increase in spending compared to 2013. Total fraud losses for the cards in the sample decreased 7 percent to 156 million pounds ($242 million).

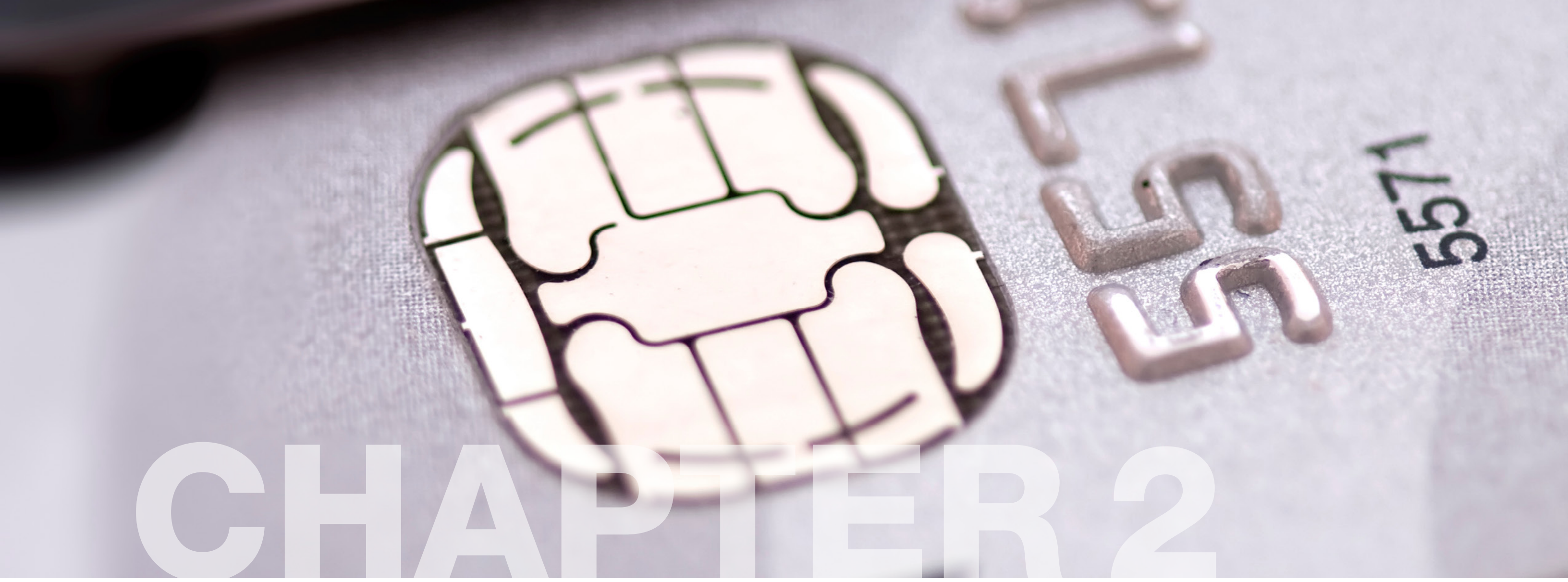
© 2015 Networld Media Group

US Tops Contries for 2014 Cross-Border Fraud on UK Debit Cards



Source: FICO

© 2015 Networld Media Group



CHAPTER 2

Attack methods

As the U.S. ATM industry migrates to EMV, new attack methods will become prevalent such as malware or black box attacks (in which a device such as a smartphone is connected to the ATM) that take control over an ATM and empty its cash; cyberattacks on FIs' card authorization systems; and explosive attacks on ATM safes rather than the traditional smash-and-grab raids.

Skimming

Skimming devices illegally record account data from the mag stripe of a credit or debit card. The device includes a card reader and a hidden camera that captures cardholder PINs.

There are three modes of ATM skimming attack: digital, analog and stereo.

According to a Triton Systems blog, "In a digital skimming attack, criminals place a device which looks like a card reader on the ATM and copy the data when the card is passed over the device. The data is typically stored in the memory of the skimmer and is downloaded to a PC where it can be read and used to make fake cards."

The blog goes on to explain that in an analog attack, "criminals record the sound of the card data signal during the transaction. The data is then retrieved from the recording and used for fraudulent purposes."

A stereo skimming attack involves a skimmer with two heads that record both the jamming signal from an anti-skimming device and the card data signal. Jamming involves creating random frequencies intended to scramble a skimmer. Stereo skimming allows the criminal to separate the jamming signal from the card data signal, which is then converted into an analog or digital format.

EAST notes that fraudsters initially used simple overlay skimmers attached to the card reader, "but with the evolution of more sophisticated types of skimming devices, the placement of them has moved to other locations around the card reader (both external and internal). Wiretapping devices (eavesdropping) have also been used to tap data at the card reader pre-read and read heads, and also card reader electronics."

To assist with the reporting and analysis of skimming devices, and to set a common standard for describing the placement of skimming and shimming (see Shimming, this chapter page?) devices, the EAST Expert Group on ATM Fraud has produced "Standardisation of Terminology for locations of Card Data Compromise devices at ATMs." The publication is available to law enforcement and EAST members and can be obtained from the organization.

EAST notes that although skimmers historically have been used used to collect magnetic stripe data, fraudsters have now developed a new generation of devices that can be used to read data from a chip (shimming) or perform a relay attack.

Even after U.S. ATMs are migrated to EMV, they will remain vulnerable to skimming attacks. This is because EMV cards still contain a mag stripe in order to remain backwardly compatible with non-EMV ATMs and POS terminals.

The ATM Marketplace white paper "Making Your ATM Secure," which is sponsored by Triton Systems, quotes Douglas Russell, founder of U.K.-based DFR Risk Management, as saying that ATM skimming remains very profitable in many regions, particularly where EMV chip cards haven't been fully adopted.

"In areas that have successfully reduced ATM skimming through EMV and anti-skimming technologies such as active jamming, criminals are forced to adapt their attack methods," Russell said. "Examples range from the relatively low-tech to the very sophisticated. The re-emergence of card-trapping fraud — where a trap is inserted within motorized card readers to allow perpetrators to physically steal consumers' cards — requires very basic tools and little skill.

"At the other end of the spectrum, miniature inlay or insert skimmers can be placed to avoid anti-skimming jamming signals, and eavesdropping techniques are gaining in popularity which involve connecting a skimming device to the actual card readers' electronics."

To combat skimming, ATM deployers should invest in anti-skimming devices from suppliers such as ACG, Diebold, TMD Security, and Wincor Nixdorf.

Major risks related to ATMs

Physical:

- vandalism, penetration, removal;
- placement of skimmers and pinhole cameras to obtain mag stripe data and PINs, which are used to produce counterfeit cards and drain customers' accounts;
- robbery of customers using ATMs; and
- robbery of service vendors visiting ATMs to deliver cash.

Cyber:

- physical access to ATM operating system to modify programming and "jackpot" the device. This involves modification to the operating system code that allows criminals to enter a series of numbers on the keypad directing the ATM to dispense money until it is empty; and
- hacking or remote access to ATMs in order to "jackpot" the machine.

Source: David Lott, payments risk expert at The Federal Reserve Bank of Atlanta Retail Payments Risk Forum. Published in "Making Your ATM Secure," an ATM Marketplace white paper sponsored by Triton Systems.

© 2015 Networld Media Group

Until all POS terminals and ATMs everywhere have migrated to EMV, the mag stripe will remain on EMV cards, making them vulnerable to skimming.

"Making Your ATM Secure" quotes Mark Smith, southeastern region sales manager at Marietta, Georgia-based Sharenet ATM, as recommending the use of ATM video surveillance to combat skimmers. "You may not be able to stop the crime in progress, but you will definitely get high-resolution photos of the criminals," he said.

Source: Triton Systems

Shimming

In August 2015, the Krebs on Security website reported that Mexican fraud experts had discovered a device known as a "shimmer" that is inserted into an ATM's card acceptance slot and used to read data directly off EMV chip-enabled cards.

In response, the ATM Industry Association issued the following statement:

"The ATMIA Security Council has been made aware that a level of confusion has arisen following extensive technical media reporting and online discussions around an apparent EMV chip card data compromise known as 'shimming.' This attack vector is only an ATM issue if the card issuers are not using EMV best practices during the transaction process."

For more information on shimming, contact the ATMIA.

Physical attacks

Smash-and-grab raids on ATMs are prevalent in the U.S. In a smash-and-grab raid, criminals break into a retail store and steal the ATM. Alternatively, they may steal cash by physically attacking the ATM's safe, using mechanical tools, torches, and gas or solid explosives to open the safe door or make an opening in the safe walls.

The ATM Marketplace white paper, "Making Your ATM Secure," quotes Sharenet's Smith as saying that, if an ATM is secured properly, criminals won't be able to remove it from the retail store.

"But many retailers take shortcuts and don't adhere to ATM manufacturers' recommendations for security," Smith said. "Therefore, some of these attacks are too easy, and the ATM is taken in seconds. It's very rare that the criminals try to break into the ATM while the raid is happening. They always take the unit and try to compromise the safe elsewhere. The damage they leave behind can exceed $30,000 in storefront destruction."

In an ATM Marketplace blog, "Smash and Grab Alive and Well," Smith recommends the following measures to ensure the physical security of retail ATMs:

- place bollards in front of stores to deter smash-and-grab raids;
- secure the ATM with bolts that can withstand vehicle impact;

© 2015 Networld Media Group

- install a digital camera at the ATM for surveillance purposes;
- add protective steel panels to make the ATM stronger, bulkier, heavier and much harder to remove; and
- install sensors that sound an alarm if an ATM is rocked off its base or exposed to extreme heat from a metal-cutting torch, or if the ATM vault is opened without authorization. The alarm can be tied in to existing systems to send alerts when a device is compromised.

Additionally, Smith advises, avoid exposing any side of the ATM to a plate glass window and install an anchoring device designed to withstand a ram raid.

> **“Criminals are very resourceful and will use all kinds of tools to try to access the cash inside an ATM, including cutting with power saws, drilling with power tools, prying with crowbars, using a torch or other burning device, using explosive gas or dynamite, and even using vehicles to drag the ATM off its base.”**
>
> Source: 3SI Security Systems

Gas attacks

Following Europe’s migration to EMV, a new type of ATM attack developed: explosive gas attacks to break open ATM safes. EAST’s second 2015 European ATM fraud report, issued in July 2015, said that 11 countries reported explosive gas attacks, and two of them reported attacks on ATMs using solid explosives.

An ATM Marketplace blog by Richard Buckle stresses that, while there have so far been no gas attacks on U.S. ATMs, ATM deployers shouldn’t assume that U.S. criminals will simply shift from skimming to cyber-attacks or identity theft following EMV deployment.

“I am extremely fearful that the greatly dumbed-down ‘blow up the ATM with gas’ model will appeal to many a would-be bad guy once the old ‘steal the ATM card’ method no longer works,” Buckle wrote.

On July 22, 2015, criminals used solid explosives to attempt to break open an ATM safe in Philadelphia, following a similar explosive attack on a Philadelphia ATM a couple weeks earlier.

Malware

Criminals can jackpot or “cash out” an ATM by installing malware on its computer by means of a CD-ROM or a USB-based “black box” device such as a smartphone, or by downloading software to the unit. Malware can be installed remotely by hacking in through an insecure connection. Once they have installed the necessary software, criminals can transmit a series of commands to the ATM to dispense all its cash without needing to use valid cards or PINs.

© 2015 Networld Media Group

To protect ATMs against unauthorized access through hacking or malware, operators need to keep their machines up-to-date with the latest security patches for their ATM applications software and operating system, and deploy firewall and anti-virus technology.

Backdoor.ATM.Suceful

ATM Marketplace reports that FireEye Labs, a threat prevention platform developer, has identified a new type of ATM malware, Backdoor.ATM.Suceful, which can retain debit cards on infected ATMs, disable alarms, and read debit card track data.

"It might still be in its development phase; however, the features provided are shocking and never seen before in ATM malware," FireEye said in a blog.

Like the earlier ATM viruses Ploutus and PadPin, Suceful interacts with XFS Manager, the interface between the application (malware, in this case) and ATM peripherals (e.g., printer, dispenser, card reader, PIN pad), ATM Marketplace says.

FireEye said in the blog that one of the most disturbing things about Suceful is that it's device agnostic:

"Every vendor has its own implementation of the XFS Manager with proper security controls in place; however, they also support the default XFS Manager template provided by WOSA/XFS standard, allowing the attackers to create their own interface with the ATM."

FireEye said that, installed in Diebold or NCR ATMs, Suceful could enable actions that include:

- reading all credit or debit card track data;
- reading smart chip data;
- controlling the malware via PIN pad;
- retention or ejection of a card on demand (used to steal cards); and
- suppressing ATM sensors to avoid detection.

"Suceful is the first multivendor ATM malware targeting cardholders, created to steal the tracks of the debit cards but also to steal the actual physical cards, which is definitely raising the bar of sophistication of this type of threat," FireEye said.

Cyber-attacks on FIs

In April 2014, the U.S. Federal Financial Institutions Examination Council warned FIs about the risk of cyberattacks on ATMs and card authorization systems.

"Cyberattacks on FIs to gain access to, and alter the settings on, Web-based ATM control panels used by small-to medium-sized institutions are on the rise," the FFIEC said.

© 2015 Networld Media Group

These attacks — which the Secret Service calls “Unlimited Operations” — result in significant losses from ATM cash-out, because they allow criminals using stolen debit, prepaid or ATM cards to withdraw funds beyond the cash balance in customer accounts or other limits typically applied to ATM withdrawals.

In a 2013 Unlimited Operations cyberattack, criminals netted more than $40 million using just 12 debit card accounts, the FFIEC said.

“The [FFIEC] members expect financial institutions to take steps to address this threat by reviewing the adequacy of their controls over IT networks, card issuer authorization systems, ATM usage parameters, and fraud detection processes,” the FFIEC said. “In addition, the members expect FIs to have effective response programs to manage this type of incident.”

The FFIEC made several recommendations:

- conduct ongoing information security risk assessments;
- perform security monitoring, prevention and risk mitigation;
- protect against unauthorized access;
- implement and test controls around critical systems regularly;
- conduct information security awareness and training programs;
- test incident response plans; and
- Participate in industry information-sharing forums.

In a Payments Journal blog post, the Federal Reserve Bank of Atlanta’s Lott recommended that FIs should address risk mitigation steps outlined in the FFIEC’s warning.

“Because the vast majority of small to mid-sized FIs depend on third-party processors to run their card management systems, it is imperative all FIs verify that their processors have the controls and safeguards in place to prevent such attacks, and they should insist on seeing validation of those controls,” he wrote.

CHAPTER 3

Security upgrades and compliance

This chapter provides an overview of EMV and PCI requirements for ATM deployers.

EMV migration

U.S.-based ATM deployers and acquirers must be ready for MasterCard's October 2016 EMV liability shift deadline for ATMs, or face the risk of fraud losses.

Migrating an ATM network to EMV involves three processes:

Firstly, ATMs must be equipped with EMV Level 1-compliant EMV motorized or dip card readers and PCI-compliant encrypting PIN pads.

As defined by EMV standardization body EMVCo, EMV Level 1 is the standard for the hardware interface enabling data transfer between EMV cards and terminals.

Secondly, ATMs must have a EMV Level 2-compliant kernel installedf. EMV Level 2 is the standard for the application software resident in the terminal that processes EMV transactions.

Thirdly, acquirers must successfully complete end-to-end EMV hardware and software testing of their entire network in order to receive EMV Level 3 certification from card networks whose cards the acquirer wishes to accept. EMV Level 3 is the standard for the entire EMV infrastructure, encompassing the terminal hardware, software and network.

The ATM Marketplace report "EMV Migration Guide" says that ATM operators who leave their EMV upgrade to the last minute could be making a costly mistake.

ATM vendors most likely will not have the resources to assist large numbers of clients trying to migrate to EMV very close to the deadline, the report says. For example, EMV card readers might be in short supply, as well as resources for EMV testing and certification.

“It costs approximately $2,000 to upgrade an ATM to be EMV-capable, which is a huge expense for a large ATM operator with a fleet of thousands of ATMs.

Source: Julie Conroy, research director for Aite Group retail banking practice

It is in a deployer’s best interests to ensure that any new ATMs include an EMV card reader, rather than a mag stripe-only device.

PCI DSS

ATM operators must comply with Payment Card Industry Security Standards Council requirements, the most important of which is the Payment Card Industry Data Security Standard.

PCI DSS includes requirements for password management, network security, firewalls, antivirus software, hardening or locking down operating systems by disabling extraneous features to prevent intrusions, and implementing system access controls.

The purpose of PCI DSS is to protect cardholder information from unauthorized access by setting enforceable standards for the quality of an organization’s information security practices.

Penalties for PCI DSS noncompliance include substantial fines by card schemes, as well as liability for fraud losses resulting from data breaches.

On April 30, 2014, the PCI SSC withdrew its approval for ATM electronic PIN pads based on version 1 of the PCI PIN Transaction Security Point of Interaction standard, i.e., PCI PTS POI V1.0. Henceforth, any ATM that is installed or moved must have an EPP that complies with the latest PCI standard for EPPs, i.e., PCI PTS POI v.3.X.

For example, a newly deployed or relocated Diebold ATM must use the manufacturer’s EPP7 PIN pad. Since May 2014, all new Triton ATMs have shipped with the company’s PCI PTS POI version 3.1-certified EPP, the T9.

For more information on PCI and EPPs, readers should contact their ATM vendor.

Windows 7

On April 8, 2014, Microsoft stopped providing updates for its Windows XP operating system. This means that ATMs that have not been upgraded from XP to Windows 7 will not receive Microsoft security patches. As a result, they will be at greater risk for malware and network intrusion, and will be in breach of the PCI DSS requirement that ATM deployers keep their operating systems updated with security patches that protect against known vulnerabilities.

However, according to the National ATM Council, the majority of the ATMs operated by American ISOs, IADs and merchants use Windows CE rather than Windows XP and are therefore unaffected by Microsoft’s end of support for XP.

In addition to updating from Windows XP to Windows 7, ATM operators should verify that they are running the latest application software from their ATM vendor, with the most recent security patches.

© 2015 Networld Media Group

CHAPTER 4

Fraud prevention technologies

This chapter provides an overview of key fraud detection and prevention technologies from ATM vendors.

ATM safe locks

To protect against theft of cash from an ATM safe (by an employee, for instance), deployers can install a safe lock.

There are two approaches to securing the ATM's internal safe:

- a combination lock requiring two people with dual access; and
- an electronic audit lock controlled by a smart key and a one-time authentication code, thus not requiring dual access.

As it is impractical to require two people to open an ATM safe, ATM operators should consider using an electronic audit lock such as the Cencon lock from Lexington, Kentucky-based Kaba Mas to safeguard their ATM safes from insider theft.

Before using the Cencon lock, an ATM cash-handler must call the dispatch center to obtain a one-time authentication code. Cencon software provides an audit trail of everyone who has accessed the ATM safe.

An alternative to the Cencon lock is the Sergeant & Greenleaf A Series audit lock, which also uses a one-time code.

"Cash Connect requires its clients to either use the Cencon lock or the Sergeant & Greenleaf A Series audit lock," said David Crossan, channel manager at Newark, Delaware-based ATM cash services company Cash Connect. "The other security advice Cash Connect gives its clients is to alert merchants and staff to watch for suspicious activity around their ATMs; to change the ATM cabinet key from the standard key that comes with the ATM to a unique key; and to consider installing a level 1 ATM safe. This is much sturdier than the business hours safe which comes as standard in most retail ATMs."

ACG

In March 2015, Alpharetta, Georgia-based ACG launched the ECS 4-in-1, which it said was the first anti-skimming solution on the market to offer combined skimming device detection and jamming protection for dip card readers.

Not only does ECS 4-in-1 sensing technology alert a deployer to ATM tampering (and deactivate the device's card reader) but also, it activates jamming technology to provide continuing protection for the cardholder.

Matthias Thiele, ACG Vice President of Global Business Development, says this "game-changing" combination is important. This is because deactivating the card reader on an ATM doesn't necessarily deactivate the skimming device, which might operate on a power source independent of its ATM host. Because the ATM will still appear to be fully functional, cardholders might attempt to use the ATM, at which point their card data can be collected by the skimmer, Thiele says.

Diebold

In September 2015, Diebold launched Site Sentry video management technology, which uses the cloud and application programming interface technology to allow clients to see and respond to security events in real time.

The new video technology is integrated into Diebold SecureStat, a cloud-based platform. Site Sentry technology turns a camera into a monitored alarm point, helping to verify alarm events, Diebold says.

Video footage can be saved to and retrieved from cloud storage exclusively — or in combination with local storage — with anytime, anywhere viewing access through SecureStat's single sign-on functionality. Video playback and analytics offer options for using video to support investigations and deliver useful business intelligence.

Diebold Site Sentry video monitoring services also are supported by the company's Central Station Alarm Association Five Diamond-certified alarm monitoring center for added support and rapid response.

"When paired with Diebold's portfolio of monitoring and managed services, Site Sentry allows our customers to maximize the investment and potential of their video surveillance program," said Felix Gonzales, Diebold electronic security vice president for strategic initiatives and business development. "By utilizing this technology, our customers will be able to proactively monitor their operations and prevent security threats."

FICO Proximity Location Service

In 2013, FICO launched a near real-time card-present fraud detection and prevention solution service for credit and debit card issuers. FICO Proximity Location Service aims to improve the security of card transactions through proximity correlation.

The solution verifies that a customer's registered mobile phone is in the same location as a flagged ATM or POS transaction, indicating a high probability that the transaction is legitmate and avoiding unnecessary inconvenience to the customer. The service can help an issuer to decide whether a cardholder account should be blocked or cleared for further activity.

"Limiting impact on subsequent transactions, FICO Proximity Location Service enhances customer service by reducing false positives, cross-border fraud and case management costs," FICO says.

FICO Proximity Location Service is provided as a cloud-based add-on to the FICO Fraud Resolution Manager service.

"Banks are trying to perfect a tricky balancing act — protect customers without causing undue frustration for cardholders who travel or who use their cards in new locations," said Gabriel Hopkins, senior director of product management at FICO. "Proximity correlation adds a powerful new tool that can help banks eliminate a great source of frustration for their customers who travel. With this service, cardholders can use their cards in other countries with significantly lower risk of being declined."

According to FICO, early client deployments have shown reductions of as much as 70 percent in standard cross-border false positive rates, helping to ensure customer satisfaction and reduce case management costs.

GMV

Madrid, Spain-based GMV offers Checker ATM Security, which helps deployers protect their ATMs from logical fraud (for example, nonphysical attacks on devices via software).

GMV says that Checker rejects unauthorized network connections, restricts access to sensitive information, prevents unauthorized devices such as USB drives from being connected to ATMs and blocks malware. Its technology combines application-level firewalls, whitelisting (allowing only approved applications), integrity verification and self-learning capabilities into enforceable ATM-specific security policies.

Checker includes centralized monitoring and management functionalities as well as ATM hard disk encryption, GMV says.

3SI Security Systems

In January 2015, Malvern, Pennsylvania-based asset protection company 3SI Security Systems introduced an ATM tracker solution that relies on GPS to locate a stolen ATM.

3SI's NextGen3 Electronic Satellite Pursuit ATM Tracker GPS leverages multiple security and tracking applications that facilitate apprehension in up to 70 percent of cases and asset return at rates of more than 87 percent, the company said.

© 2015 Networld Media Group

According to 3SI, the compact profile of ATM Tracker accommodates easy installation in different types of ATMs. Other features of the new product include:

- configuration options that allow the device to trigger on ATM tilt and motion or just tilt;
- dual internal and external GSM and GPS antennas;
- input-output options to detect a breach or activate a siren or strobe;
- an RF beacon that pinpoints the location of the tracker to make apprehension of criminals easier;
- data storage that improves tracking reliability by allowing automatic data retrieval if the cell connection is lost; and
- a daily network and battery health check.

In July 2015, 3SI launched SecuriDab LT, a solution designed to protect ATMs against physical attacks. This solution includes a general control unit and up to four ink-staining devices. The GCU acts as the "brain" for the system and, when an attack is detected, communicates with the staining devices. The system uses a multiphase activation method to: (a) indelibly stain the notes in the cassette during a real attack; and (b) protect against accidental activation.

3SI says SecuriDab LT is flexible in what it can sense, including: tilt from a pull-out attempt; high impact blast from a solid explosive or gas attack; temperature increase from a blow torch attack; light from a breach; and input from external systems such as alarms, locks, and tracking units. Also, the unit can be optionally equipped with explosive gas neutralization technology to prevent damage from a gas attack.

TMD Security

Schaffhausen, Switzerland-based TMD Security provides technology to combat skimming. TMD offers a range of Security Packs, each of which is based on its Card Protection Kit (CPK+) core technology, enabling customers to select from flexible combinations of complementary protection.

In March 2015, TMD launched a solution that continuously defends against skimming attacks on dip card readers without taking the ATM out of service. The company's Active DIP Kit generates multiple random electromagnetic signals (i.e., jamming) to prevent the copying and deciphering of data stored on the card's mag stripe. The cardholder experience is unaffected and, because card data is always protected by ADK, the ATM can safely remain in service throughout an attack, TMD said.

TMD introduced jamming protection in 2004 but, until the launch of ADK, it only offered continuous active protection to motorized card readers. Jamming could be activated for dip readers only upon the detection of a skimming device, at which time the ATM or self-service terminal would need to be taken out of service.

"Many motorized ATMs are now actively protected, so dip card readers are exposed and increasingly targeted for skimming," said TMD CEO Cees Heuker of Hoek.

Trusted Security Solutions

Harrisburg, North Carolina-based Trusted Security Solutions provides secure ATM key management solutions for organizations that manage cryptographic keys. Its A98 ATM initial key establishment system includes the A98-R platform, which offers remote key loading to automte the generation and distribution of cryptographic keys for ATMs and eliminate on-site manual key loading.

Most networks and standards groups consider remote key loading to be more secure than traditional methods that use paper key components and the concept of dual person control or split knowledge to maintain compliance, Trusted Security Solutions says.

Wincor Nixdorf

Wincor Nixdorf's PC/E Terminal Security platform offers the following features:

Access protection

Many features of Microsoft operating systems such as Windows XP and Windows 7 aren't required for ATM use, and are potential weaknesses that can be exploited by hackers.

Access protection hardens the operating system by disabling or removing superfluous components and services and reducing the "attack surface." The feature also secures login processes and restricts remote access, making it harder to exploit security settings.

Intrusion protection

This feature protects ATMs against all forms of malware, not by removing them from the operating system as Microsoft "scrubber" programs do, but by preventing their installation in the first place.

Intrusion protection continuously monitors for any change or anomaly within an ATM's programs or behavior. It protects not only against external attacks, but also against internal threats such as rogue programmers or service branch employees attempting to manipulate ATM behavior.

Hard disk encryption

The HDE feature in PC/E Terminal Security Software minimizes the risk of manipulation, misuse or theft by encrypting the contents of the ATM's hard drive, making it unreadable not only in a case of unauthorized boot-up but also in the event of the theft of the ATM's internal PC or hard disk.

The solution works by encrypting unique identifiers for each of the ATM's peripherals — e.g., card reader, PIN pad, printer, and cash dispenser. "When you install [PC/E Terminal Security Software], it encrypts the disk with this information," Wincor Nixdorf Senior Trusted Advisor Terence Devereux told ATM Marketplace. "So, if I remove the disk from the ATM, because these devices aren't there, you don't gain access to the disk."

Optical Security Guard

This feature operates with optical sensors to monitor ATMs and prevent tampering attacks such as skimming and card trapping. It is based on smart image analysis software that interacts with cameras on the customer panel and card entry slot to continuously analyze the ATM state. If modifications to an ATM are detected, the solution triggers an alarm and, if applicable, stops further transactions.

ProView Video Surveillance

This solution reduces the risk of ATM vandalism and transaction fraud. Cameras mounted on the ATM record cash transactions from start to finish, preventing many types of fraud and transaction manipulation. These stored images or video footage are helpful both in spotting criminals trying to alter the device and in identifying scams such as transaction reversal fraud.

ProView Video Surveillance software offers both centralized image and video monitoring and image analysis.

Fraud prevention

This feature uses the real-time multichannel IRIS solution by Iris Analytics to prevent and combat fraud and to control risk for all types of card-based payments. IRIS is able to detect, in real-time, specific types of ATM attacks such as skimming and transaction reversal fraud.

Terminal Security and Windows XP — End of life

This feature is designed to protect ATMs still using Windows XP from data theft, cyber-crime and malware. It helps harden the operating system with a wide range of intrusion and access protection controls.

© 2015 Networld Media Group

CHAPTER 5

Recommendations

This chapter provides recommendations for physical and logical ATM security.

The onion-layer approach

According to Terence Devereux of Wincor Nixdorf, ATM deployers should implement tightly integrated security layers that comprise the “onion” approach to protecting ATMs, operating systems, and customer data. During an ATM Marketplace webinar in February 2015, Devereux said this model ensures that, if one security layer fails, others will take over to shield and secure an organization’s critical assets.

“Securing ATMs and POS devices isn’t just about preventing monetary losses — it’s also about protecting something far more valuable, which is your customer’s trust,” Devereux said. “A smart way to deliver [physical and logical] security is by implementing a layered, onion approach that can catch continuously evolving threats.”

Part of Wincor’s 365-degree security concept for self-service systems, the onion model includes nine tenets:

1. protect against unauthorized boot-up and hard disk access via CD-ROM or USB drives;
2. allow only authorized incoming and outgoing communications;
3. encrypt all communications using SSL/HTTPs;
4. ensure transaction integrity through message authentication codes that validate transaction communications between the ATM and the host server or switch;
5. follow PCI DSS “need to know” and “need to have” principles for controlling ATM access, and harden the ATM operating system;
6. implement defences against unauthorized use of system resources;
7. employ file integrity management for designated operation-critical system files and payment applications;

8. use behavioral monitoring to recognize anomalous patterns in systems and transactions;
9. safeguard cardholder data by masking or encrypting the information and never displaying, storing, or transmitting it in the clear.

Source: Wincor Nixdorf

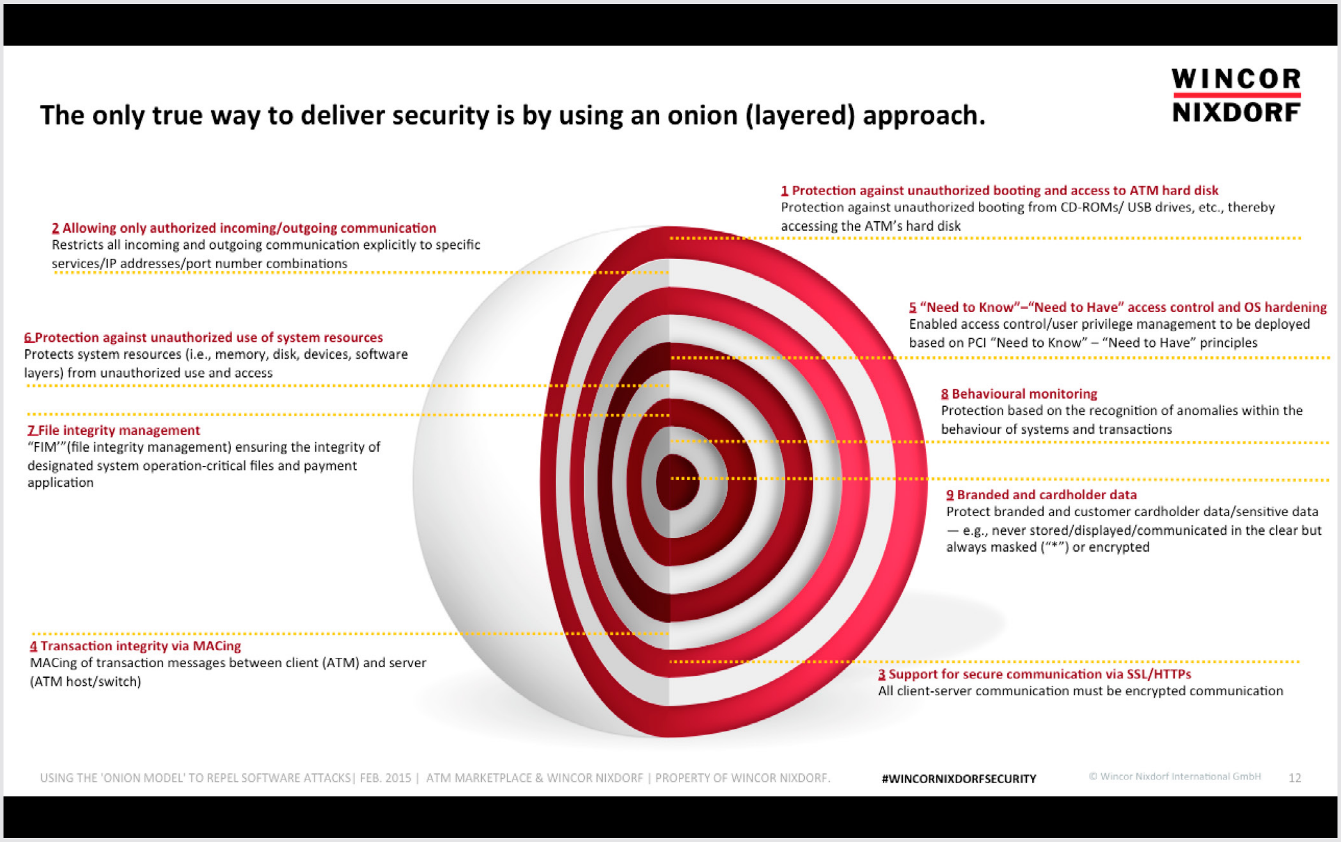
Advanced Security Module

On Triton's atmAToM.com blog, Cornell wrote that ATMs should be equipped with an Advanced Security Module, to prevent "man-in-the-middle" attacks — that is, issuing instructions directly to the ATM dispenser in order to empty the machine of cash.

"Triton's ATMs have always included a security module to defend against this class of attack," Cornell wrote. "But the Advanced Security Module takes this defense to a different league."

Henry Schwarz, Triton software projects director, wrote in an atmAToM.com blog that Triton's Advanced Security Module resides within the ATM's vault between the ATM controller and the

The onion layered approach



The only true way to deliver security is by using an onion (layered) approach.

WINCOR NIXDORF

1 Protection against unauthorized booting and access to ATM hard disk
Protection against unauthorized booting from CD-ROMs/ USB drives, etc., thereby accessing the ATM's hard disk

2 Allowing only authorized incoming/outgoing communication
Restricts all incoming and outgoing communication explicitly to specific services/IP addresses/port number combinations

3 Support for secure communication via SSL/HTTPs
All client-server communication must be encrypted communication

4 Transaction integrity via MACing
MACing of transaction messages between client (ATM) and server (ATM host/switch)

5 "Need to Know"–"Need to Have" access control and OS hardening
Enabled access control/user privilege management to be deployed based on PCI "Need to Know" – "Need to Have" principles

6 Protection against unauthorized use of system resources
Protects system resources (i.e., memory, disk, devices, software layers) from unauthorized use and access

7 File integrity management
"FIM'"(file integrity management) ensuring the integrity of designated system operation-critical files and payment application

8 Behavioural monitoring
Protection based on the recognition of anomalies within the behaviour of systems and transactions

9 Branded and cardholder data
Protect branded and customer cardholder data/sensitive data — e.g., never stored/displayed/communicated in the clear but always masked ("*") or encrypted

USING THE 'ONION MODEL' TO REPEL SOFTWARE ATTACKS| FEB. 2015 | ATM MARKETPLACE & WINCOR NIXDORF | PROPERTY OF WINCOR NIXDORF. #WINCORNIXDORFSECURITY © Wincor Nixdorf International GmbH 12 cash dispenser. The module cryptographically authenticates commands sent to the cash dispenser, ensuring that they were issued by a legitimate ATM controller and not by an interloper using a “black box” device such as a smartphone connected to the ATM.

Best practice

Cornell’s atmAToM.com blog caution’s ATM deployers not to use default ATM passwords and to ATM passwords regularly.

Active encryption key management also reduces the risk of ATM attack. The PCI DSS mandates that ATM deployers update keys at least annually. Instead of the cumbersome and error-prone key management process of changing master keys on ATMs with two technicians and dual sets of keys, Cornell recommends using remote key technology, which eliminates these physical visits altogether.

ATM deployers should use message authentication codes to verify that messages between an ATM and a host are authentic and unmodified, thus preventing “man-in-the-middle” attacks. “The message validation occurs through a set of keys supplied by the processor and installed on your ATMs,” Cornell wrote. “Contact your processor to find out how to enable MAC-ing on your ATMs.”

Triton says that when TCP/IP communications are used, SSL should be enabled on both the server and the ATM, allowing the machine to authenticate the host server, and ensuring message encryption and integrity between host and ATM (either hard-wired or using a wireless connection).

Biometric authentication

Traditionally, ATMs have required customers to authenticate themselves via card and PIN, a method that is vulnerable to fraud. Although not a new technology, biometric authentication offers a solution to the problem of authenticating customers without introducing friction into the transaction process.

According to a blog by Robert Johnston, NCR marketing director for ATM software, biometric technology has been widely adopted for ATMs in Japan and Latin America.

Oftentimes, an ATM deployer will install a fingerprint scanner that works in conjunction with a card reader and PIN pad, although biometric authentication can be used to replace the card and PIN.

Fingerprint authentication must work reliably in difficult real-world conditions, ensure proof of presence, and prevent the use of fake fingerprints or biometric “spoofs,” Phil Scarfo, vice president of global marketing for biometrics at HID Global, wrote in an ATM Marketplace commentary.

“HID Global has addressed these challenges with Lumidigm sensors featuring multispectral imaging technology,” Scarfo wrote. “These sensors use multiple sources and types of light along with advanced polarization techniques to reach all the way down to capillary beds and other subdermal structures to collect truly relevant fingerprint data. The technology also includes field-updatable liveness detection capabilities to ensure that real human tissue can be identified as authentic within a fraction of a second — an important consideration at ATMs.”

© 2015 Networld Media Group

"When managed correctly and coupled with intelligent encryption-enabled and tamper-resistant devices, biometric authentication is secure and requires no more than the touch of a finger to assure an FI that an authorized account-holder is actually present at its ATM."

Another option is to allow customers to make cardless cash withdrawals via smartphone, using a fingerprint sensor such as Apple Touch ID to authenticate themselves on their mobile device.

In April 2015, U.S. financial software vendor FIS launched biometric authentication for its mobile banking application via Touch ID. The technology allows bank or credit union customers to authenticate themselves to the FIS Cardless Cash application via fingerprint. FIS developed the software in partnership with Paydiant.

"One-touch Cardless Cash is unlike anything else in the market," said Douglas Brown, senior vice president and general manager of mobile financial services at FIS. "The ability to access your account and withdraw money with just your fingerprint will make ATM access faster, safer and easier for users."

In addition, ATM users can be authenticated by facial recognition technology, which uses the device's front-facing camera to identify accountholders through image-matching before allowing them to complete a transaction.

FICO recommendations to FIs:

- Increase security around all ATM equipment. Consult local law enforcement to coordinate police involvement for increased patrols and surveillance.
- Make an extra effort to examine the front of every ATM for unusual attachments that may be disguised as native equipment. In addition, check loose ceiling tiles above ATMs for hidden cameras or transmitters.
- Examine the ATM's façade for sticky tape or Velcro residue, which could indicate that an ATM parasite was attached to the machine previously.
- Keep a photo file of ATM equipment to aid in physical security inspections.
- Test all video equipment to ensure that it is in working order and properly archived in case it is needed to pinpoint card skimming time ranges using surveillance records.

Following a suspected skimming incident, contact local law enforcement and FICO Card Alert Service. Prior to the call, gather any available data, such as terminal ID, address and suspected skimming date ranges.

Source: FICO Card Alert Service

© 2015 Networld Media Group

SUPPLIERS

ATM Marketplace
www.atmmarketplace.com

"Find Suppliers" pages
http://www.atmmarketplace.com/companies/directory/
http://www.atmmarketplace.com/companies/directory/products-and-services/security/
http://www.atmmarketplace.com/companies/directory/products-and-services/bank-security/
http://www.atmmarketplace.com/companies/directory/products-and-services/emv/

3SI Security Systems
https://www.3sisecurity.com/
https://www.3sisecurity.com/industries-solutions/industries/atm/
http://www.atmmarketplace.com/companies/media/3si-security-systems/

U.S. contact
info@3sisecurity.com
101 Lindenwood Drive, Suite 200
Malvern, PA 19355
Tel. 1 800 523 1430

ACG
ATM parts repair and anti-skimming technology
www.acgworld.com
5010 McGinnis Ferry Rd., Suite A
Alpharetta, Georgia 30005 U.S.
http://www.atmmarketplace.com/companies/media/acg-trusted-provider-to-financial-institutions/?type=asset
Tel. 1 800 536 5085
Email: sales@acgworld.com

Clear2Pay, an FIS company
http://www.fisglobal.com/products-opentestsolutions

Clear2Pay EMV solutions and services
http://www.atmmarketplace.com/companies/showcases/clear2pay/products/emv-solutions-and-services/

FIS
http://www.fisglobal.com/
601 Riverside Avenue
Jacksonville, FL 32204 U.S.
General Information: 1 904 438 6000
Toll-free (U.S. only): 1 888 323 0310
Global Mid-tier & Large Banking: 1 501 220 4999
E-mail: moreinformation@fisglobal.com

Diebold
http://www.diebold.com
http://www.atmmarketplace.com/companies/showcases/diebold-incorporated-2/

Security solutions
Tel. 1 855 331 0359

FICO
www.fico.com
Corporate Headquarters
181 Metro Drive
San Jose, CA 95110 U.S.
Tel.1 408 5351500

FICO fraud prevention solutions
Tel. 1 888 342 6336

FTSI, Inc.
https://www.ftsius.com/
406 E. Huntington Drive, Suite 100
Monrovia, CA 91016 U.S.
Tel. 1 818 241 9571
Email: info@ftsius.com
ATM and branch security solutions
http://www.atmmarketplace.com/companies/showcases/ftsi/products/atm-branch-security-solutions/

GMV
http://www.gmv.com/en/
http://www.gmv.com/en/BankingandInsurance/
http://www.gmv.com/export/sites/gmv/DocumentosPDF/SeguridadInfo-Documentacion/Checker_ENG-15-01-2013.pdf
Isaac Newton, 11 P.T.M. Tres Cantos, 28760 Madrid, Spain
Email: marketing.TIC@gmv.com
Tel. +34 918072100
http://www.atmmarketplace.com/companies/showcases/gmv/

KAL ATM Software
www.kal.com
John Cotton Building
Sunnyside, Edinburgh
EH7 5RA U.K.
Tel. +44 131 659 4900
Email: info@kal.com

KAL EMV compliance solutions
http://www.atmmarketplace.com/companies/showcases/kal-atm-software/products/kal-emv-compliance-solutions/

NCR
http://www.ncr.com/
Tel. 1-800-Call-NCR

NCR security solutions
http://www.atmmarketplace.com/companies/showcases/ncr-financial-solutions/products/ncr-atm-security-solutions/
http://www.ncr.com/financial-services/ncr-secure
“Have You Done All You Can To Secure Your ATM Network?”
NCR white paper
http://www.atmmarketplace.com/whitepapers/have-you-done-all-you-can-to-secure-your-atm-network/

Paragon Application Systems
Software to test the integrity of ATMs and POS systems
http://www.paragonedge.com/
326 Raleigh Street
Holly Springs, NC 27540 U.S.
Tel. 1 919 567 9890
Email: info@paragonedge.com
http://www.atmmarketplace.com/companies/showcases/paragon-application-systems/
Online EMV and payments training classes from Paragon Application Systems
http://www.atmmarketplace.com/companies/showcases/paragon-application-systems/products/emv-and-payments-online-training-classes-from-paragon-application-systems/

SPL Group
http://spl-group.com/
SPL Computer Trading GMBH
Industriestrasse 32
49565 Bramsche Germany
Tel. +49 5461 88278 100
Email: info@spl-group.com

SPL Group USA, Inc.
2050 North Andrews Ave. #103
Pompano Beach, FL 33069 USA
Tel. 1 954 978 6720
Email: information@spl.net
www.spl.net

Security products
http://www.atmmarketplace.com/companies/showcases/spl-group/products/security-products-2/
TMD Security GMBH
Anti-skimming technology vendor
http://www.tmdsecurity.com/

Rheinweg 1
8200 Schaffhausen
Switzerland
Netherlands-based global support center
Tel. +31 36 751 94 00

TMD Security North America
Tom Moore, Managing Director North America
Tel. 1 215 431 4734
http://www.atmmarketplace.com/companies/showcases/tmd-security-gmbh/

Triton Systems
www.triton.com
www.tritonatm.com
Triton customer support, parts, service and training are available at ATMGurus.com
For Triton’s security recommendations, see http://www.atmgurus.com/support/security-faq
21405 B Street, Long Beach, Mississippi 39560 U.S.
Tel. 1-866-7-TRITON (1-866-787-4866)
Tel. 1 228 575 3100

ATMGurus.com
Tel. 1-888-7-ATMGurus (1-888-728-6487)
Tel. 1 228 575 3175

Trusted Security Solutions
http://www.trustedsecurity.com/
838 Highway 49 South
Harrisburg, NC 28075 U.S.
Tel. 1 704 849 0036
Email: info@trustedsecurity.com
http://www.atmmarketplace.com/companies/showcases/trusted-security-solutions-inc/

Wincor Nixdorf
http://www.wincor-nixdorf.com/internet/site_EN/EN/Home/homepage_node.html
http://www.wincor-nixdorf.com/internet/site_At/EN/Products/Software/Banking/ProClassicEnterprise/Security/PCETerminalSecuity/PCETerminalSecuity_node.html

Wincor Nixdorf USA
http://www.wincor-nixdorf.com/internet/site_AT/US/Home/homepage_node.html?__site=US
12345 N. Lamar Blvd., Suite 200
Austin, Texas 78753 U.S.
Tel. 1 512 676 5000
Email: info.us@wincor-nixdorf.com

REFERENCES

ATM Marketplace
www.atmmarketplace.com

http://www.atmmarketplace.com/topics/emv/

Money mules a stubborn problem for ATM operators
http://www.atmmarketplace.com/articles/money-mules-a-stubborn-problem-for-atm-operators/

The chicken, the egg and the chip card
http://www.atmmarketplace.com/articles/the-chicken-the-egg-and-the-chip-card/

6 ATM anti-fraud steps for small FIs
http://www.atmmarketplace.com/articles/6-atm-anti-fraud-steps-for-small-fis/

Webinar: ATM security - Using the ‘onion model’ to repel software attacks, sponsored by Wincor Nixdorf
http://www.atmmarketplace.com/whitepapers/live-webinar-atm-security-using-the-onion-model-to-repel-software-attacks/

Serving the user, securing the ATM: A delicate balance, webinar sponsored by TMD Security
http://www.atmmarketplace.com/articles/tmd-webinar/

How crime can undermine the convenience of cash, white paper sponsored by Wincor Nixdorf
http://www.atmmarketplace.com/whitepapers/how-crime-can-undermine-the-convenience-of-cash/

“How to Profit from ATMs: A Guide for Retailers and Restaurateurs” by Robin Arnfield
ATM Marketplace report sponsored by Elan Financial Services
http://www.atmmarketplace.com/whitepapers/how-to-profit-from-atms-a-guide-for-retailers-and-restaurateurs-2/

ATM Marketplace ATM security white papers
http://www.atmmarketplace.com/topics/security/whitepapers/

“Making Your ATM Secure” by Robin Arnfield
ATM Marketplace white paper sponsored by Triton Systems
http://www.atmmarketplace.com/whitepapers/making-your-atm-secure/

ATM Marketplace EMV white papers
http://www.atmmarketplace.com/topics/emv/whitepapers/

“Best Practices for EMV Migration”
ATM Marketplace white paper by Robin Arnfield, sponsored by National Cash Systems
http://www.atmmarketplace.com/whitepapers/best-practices-for-emv-migration/

ATM Marketplace skimming/fraud white papers
http://www.atmmarketplace.com/topics/skimming-fraud/whitepapers/

© 2015 Networld Media Group

Infographic: ATM Skimming: Modern-Day Bank Robbery, sponsored by Diebold
http://www.atmmarketplace.com/static_media/filer_public/68/00/6800c9ca-d10d-4b1c-a163-3f0ea6635a4b/diebold-atm-skimming.pdf

“ATM Cash Management 101” by Robin Arnfield
ATM Marketplace report sponsored by Cash Connect
http://www.atmmarketplace.com/whitepapers/atm-cash-management-101/

“EMV, PCI and the ATM Industry” by Robin Arnfield
Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/8593/17477

“EMV Migration Guide” by Robin Arnfield
Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/8593/17226

“Windows 7 ATM Migration Guide” by Robin Arnfield
Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/8593/16674

“Mobile Banking and Payments Security” by Robin Arnfield
Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/12036/18751

“Mobile Payments Security 101” by Robin Arnfield
http://www.mobilepaymentstoday.com/whitepapers/mobile-payments-security-101/

atmAToM.com, Triton’s ATM industry blog
www.atmatom.com
http://www.atmatom.com/category/security/

ATM Industry Association
www.atmia.com

ATM Security Association
http://atmsecurityassociation.com/

EMV Connection
http://www.emv-connection.com/emv-faq/
http://www.emv-connection.com/implementing-emv-at-the-atm-requirements-and-recommendations-for-the-u-s-atm-community/

EMVco
https://www.emvco.com/

European ATM Security Team
https://www.european-atm-security.eu/
https://www.european-atm-security.eu/industry-information/atm-crime-definitions/

National ATM Council
www.natmc.org
9802-12 Baymeadows Road # 196
Jacksonville, Florida 32256 U.S.
Tel: 904-683-6533
mail@natmc.org

PCI Security Standards Council
https://www.pcisecuritystandards.org/

© 2015 Networld Media Group