A guide from ATMmarketplace.com

Anti-skimming Technology and EMV for the ATM

Card skimming is the No. 1 ATM security issue, and threatens to increase in the United States. Fortunately, strategies exist to combat the crime.

Developed and published by

atm marketplace

Sponsored by

TMDSECURITY
ANTI-SKIMMING TECHNOLOGY

Contents

Anti-skimming Technology and EMV for the ATM

About the sponsors

***TMD Security GMBH**, based in Schaffhausen, Switzerland, developed the first Card Protection Kit in 2004. In 2009, the new CPK + 6000 was released as the most advanced anti-skimming solution ever. TMD also offers premium protection service, which provides 24/7 monitoring of the CPK and other critical transactional parts. TMD has established OEM relationships with leading manufacturers and value-added resellers around the world.*

***ATMmarketplace.com**, owned and operated by Louisville, Ky.-based NetWorld Alliance, is the world's largest online provider of information about and for the ATM industry. The content, which is updated every business day and read by business and industry professionals throughout the world, is free.*

Published by NetWorld Alliance.

Written by **Gary Wollenhaupt**, contributing writer, ATMmarketplace.com.
Updated by **Richard Slawsky**, contributing editor, ATMmarketplace.com.
Dick Good, CEO
Tom Harper, president and publisher
Andrew Davis, senior vice president, sales and marketing
Joseph Grove, vice president and executive editor

Chapter 1 ATM skimming fraud overview

By Gary Wollenhaupt
Contributing writer, ATMmarketplace.com

Despite the concerted efforts of financial institutions around the world, ATM skimming fraud continues to be a growing problem. Skimming occurs when criminals "skim," or steal, data from the magnetic stripe on an ATM card during a transaction, usually without the cardholder's knowledge.

Skimming is a technologically sophisticated crime, requiring a technologically sophisticated response.

The criminals must devise and place an electronic card-reading device on an ATM, and observe the customer's PIN in some fashion, usually with a small camera, with a false PIN pad or by simply looking over the user's shoulder. With that data, crooks can withdraw cash from that customer's account, clone new debit and credit cards and sell the personal information to other criminal organizations.

The total scope of ATM skimming fraud is difficult to track. Nearly 70 percent of financial institutions who responded to a survey conducted by anti-fraud firm Actimize said they had experienced an increase in ATM/debit card fraud claims in 2008 compared with 2007, and those numbers were expected to increase in 2009. High-profile security breaches have focused attention on the issue. For instance, President Barack Obama cited the RBS WorldPay breach, in which thieves withdrew $9 million in 30 minutes, as the type of crime targeted by the United States' cyber-security initiative.

Recent headlines include New York City's Sovereign Bank losing more than $500,000 to skimmers, while a Romanian farmer was jailed in Australia for skimming $33,000 in that country.

What's distressing is those are only the losses that have been reported. The unknown, or at least unpublicized, losses are likely much larger. No financial institution is immune. Losses due to card skimming occur essentially everywhere ATMs are deployed around the world.

The European ATM Security Team (EAST) reported an 8 percent rise in ATM-related fraud attacks in 2009, in addition to a 149 percent rise in similar fraud attacks during 2008. Card trapping rose by 209 percent — increasing from 701 incidents in 2008 to 2,166 incidents in 2009 — while the total number of skimming incidents reported decreased by 1 percent over the same period.

Swiping a card at an ATM can leave the cardholder vulnerable to criminals who steal data from the magnetic stripe.

 | Sponsored by TMD Security

However, despite the increase in incidents, EAST reported a 36 percent drop in ATM-related fraud losses in 2009, with total reported losses of €312 million ($400 million US), down from €485 million ($622 million US) in 2008. Annual losses due to card skimming have fallen for the first time since EAST began tracking them in 2004, down from €484 million ($620 million US) in 2008 to €310 million ($397 million US) in 2009.

ATM skimming, however, remains a primary security issue in the European Union, despite the wide launch of EMV/chip-and-PIN technology, EAST officials say.

The ATM Industry Association launched an international anti-skimming forum to support the industry's response to the threat.

"Just over 4,500 of the 11,360 ATM crimes recorded on our global Cognito crime data management system for the 2005-2008 period involve skimming," Mike Lee, CEO of ATMIA, said in announcing the forum. "It's probably the most widespread crime type we face."

Protecting against skimming attacks has become a battle of wits with organized gangs of criminals. Unfortunately, stopping the activity in one place simply shifts criminal activity to other locations.

In the fight to stop skimming, one often-overlooked factor is that skimming is essentially a two-part crime. First, the customer's card data is stolen. Then, usually at a later time, the stolen data is used to withdraw cash or buy goods, often in another city, another country or online. So the thieves have to be technologically savvy enough to consummate both transactions, or have partners that can use the data.

Ultimately, stopping or even significantly slowing skimming activity will require attacking both steps in the process. Back-office systems that monitor card-usage patterns can help to detect fraudulent activities, stopping the payouts using the data from the skimmed cards.

"Banks have to protect the data from getting stolen, but the most significant measure that banks can take is to step up fraud detection systems to stop the payouts," said Avivah Litan, vice president and distinguished analyst at Gartner Inc., a Stamford, Conn.-based technology research and advisory company.

Litan promotes a multilayered approach to security that encompasses the entire ATM payment chain. But it's not that easy.

"Banks should buy new ATMs with anti-skimming devices, issue new cards with fingerprint technology and have back-office fraud systems that detect suspect patterns of behavior," she said. "But unfortunately, I don't know any banks that can afford to do all of that right now."

Card trapping a growing threat

EAST first reported an increase in card-trapping incidents at the end of the first six-month period in 2009, and the figures for the second six months have shown a further increase. A new type of card-trapping device also has been reported,

although most such devices remain fairly unsophisticated. Card-trapping incidents using the so-called "mousetrap" device were reported by four countries.

Card trapping uses a device placed in the ATM's card slot to "trap" the customer's card inside the machine. One such trapping method, the "Lebanese loop," uses tape, wire or thread to trap a card after it has been inserted. A thief observes the customer entering his PIN and retrieves the card once the customer has departed.

A number of vendors have introduced products designed to thwart card trapping. Some products detect the presence of a trapping device and prevent the customer from inserting his card. Card trapping is an old type of crime that was re-introduced by criminals after skimming attempts became more complicated due to increased security on the ATM.

One method of security is attached to existing card readers. Swiss-based TMD Security developed its Anti Trapping Kit, ATK, which is a multivendor solution that triggers on predefined conditions. Once triggered, the card is locked inside the card reader and can be released only by the ATM operator physically removing the card.

Despite the advances in anti-trapping technology, security experts still warn customers to immediately notify their bank if their card is not returned following a transaction.

Regional scope

Over the past several years, card skimming has become a global issue as criminals search out vulnerable areas. Cases have been reported in Asia-Pacific, the Americas, Africa, Russia and the Middle East, as well as in Europe.

Card trapping uses a device placed in the ATM's card slot to "trap" the customer's card inside the machine.

Adoption of EMV chip-and-PIN technology to thwart skimming has, in some cases, shifted the scope of operations. Actual skimming of card data has dropped significantly in most regions that have adopted EMV, including many countries in the Single Euro Payments Area. However, EMV has separated the two halves of the criminal transactions, as criminals may steal magnetic stripe information in one country that requires EMV, which may make it impossible to withdraw cash there.

If that happens, the criminal organization shifts the withdrawal transaction to a vulnerable area.

"The EMV rollout in Europe continues to be effective, although international losses are expected to continue while criminals are able to illegally withdraw cash from ATMs abroad that are not EMV compliant," said Lachlan Gunn, EAST director and coordinator.

Anti-skimming technology overview

This guide offers an overview of the major anti-skimming technology available in the

marketplace today, including the EMV cards that are in use in many parts of the world.

Talking about ATM security raises difficult issues: Many in the industry are afraid to discuss anti-skimming in great detail in publicly available forums for fear of giving information to criminals.

Therefore, this guide is necessarily circumspect in regard to some of the technological details.

Types of anti-skimming technology

ATM physical security. One approach to protecting against skimming attacks is to deny criminals access to card data. That means fortifying the ATM to detect and alert financial institutions of fraudulent activity at the ATM. Various technologies have arisen that make it virtually impossible to place skimming devices at ATMs, or at least force the criminals to take extreme measures to have a chance of success. These systems also can work in conjunction with monitoring and alert systems that can direct security or service personnel to the affected ATM location. Video monitoring can provide fast response to an alert, and also can help avoid expensive responses to false alarms.

ATM software security. Software, both on the ATM and in back-office operations, is perhaps the strongest line of defense against skimming attacks and fraudulent payments. However, software also is vulnerable to compromise, especially from people within an organization, such as employees, or supposedly trustworthy partners, such as service personnel or consultants. Often, software will provide the first indication of a skimming attack, but false alarms may lessen the sensitivity to alerts.

From a more systemic approach, financial institutions can stop fraudulent payments with pattern recognition software that recognizes and stops criminals' transactions.

With a large number of compromised cards in circulation already, criminals may be able to use the data in hand to withdraw money even if the flow of newly compromised cards comes to a halt.

User security. Customers can play a significant role in protecting their card data and their bank accounts, but it requires a higher level of awareness than is common today. However, financial institutions are understandably reluctant to alarm their customers. ATMs may bear warnings about guarding PINs, and even sport mirrors to ensure that no one is standing close enough to see the PIN pad. But all too often, customers aren't aware of the history of attacks within a city or at a particular location. Sophisticated skimming devices that expertly mimic the ATM fascia would fool anyone but an expert.

Certainly, customers can play a role in protecting their card data, but the onus is on the industry to provide the tools.

EMV technology. EMV, also known as "chip and PIN," is an industry standard for smart cards and card readers. It takes its name from Europay, MasterCard and Visa, the three card brands that originally supported its development. EMV cards contain a computer chip that carries cardholder data. However, during this transitional phase in countries that have adopted EMV, the magnetic stripe continues to be in use as well, which has compromised security in some cases.

Chapter 2 ATM physical security

American gangster John Dillinger had an easy answer to the question of why he robbed banks. "Because that's where the money is," he quipped.

There's a similarly simple reason why criminals around the world target ATM and debit cards: It's easy.

"The biggest weakness on the card is the magnetic stripe, and, as far as the bad guys are concerned, it's a transparent technology," said Graham McKay, consultant for the European division of ATMIA.

With increasing sophistication, criminals are able to mimic the appearance of ATM fascias, card readers and other aspects that fool all but the most observant users. They may make card readers that fit over the card slot in the ATM, or place very small readers in the legitimate card slot.

Not long ago, the skimmers were ugly, clunky add-ons that gave themselves away. They often didn't fit right, and looked as if they were made in a basement workshop. But that's not the case anymore.

"Some criminals are machining their skimmers and they are as good as the original manufacturer's bezels," said Steve Bruno, vice president of financial solutions development and support for Nautilus Hyosung America Inc., a Coppell, Texas-based technology leader of self-service solutions in hardware, software and banking services to the financial industry.

Of course, the data from the magnetic stripe is useless without the corresponding PIN data. Thieves use a variety of approaches to gain that information, especially now that customers have been educated to guard their PIN.

Some ATM installations have installed mirrors to ensure that no one shoulder surfs for the number, looking over the user's shoulder to see the pad. Most customers are well aware of that scam, and ATM etiquette has developed so that people in queue to use the machine stand far enough back to ensure privacy.

Because customer education has all but done away with shoulder surfing, thieves have adopted a more technological approach. A common way to snatch PINs is with a small camera, hidden from sight, with a view of the PIN pad.

European Payments Council anti-skimming recommendations

- Design ATM card readers to prevent attachment of skimming devices
- Install measures for the identification, jamming or disturbing of skimming devices already attached to an ATM
- Send alerts when an ATM is tampered with
- Install privacy shields to hide customers' hands as they input PINs
- Display warnings about skimming devices and available incident report channels on or near the ATMs
- Install anti-skimming devices on ATMs that have been previously targeted and compromised by criminals

Source: European Payments Council

In a recent skimming attack in New York, the criminals affixed a mirror to the face of the ATM, ostensibly to help guard against shoulder-surfing attacks. However, hidden in the mirror mount was a small pinhole camera aimed at the PIN pad. Customers were lulled into feeling they were safe at that ATM, thanks to the security precaution of the mirror.

To provide protection for the ATM, a number of defensive technologies have been developed. Some are being integrated as standard equipment in new units, while other protection is available for upgrading legacy machines.

Depending on the extent of the upgrades and the size of the ATM portfolio, adding anti-skimming devices can be an expensive proposition. From a systemic view, fortifying one section of the ATM network may simply shift the problem to another area. But each financial institution and ATM operator must look out for its own security first.

The multitude of ATM choices available to customers means they may use a vulnerable machine and not know it.

"A bank can't upgrade all the ATMs because the bank doesn't own them all and a consumer can use any ATM they want," said Gartner's Litan. "But that doesn't mean a bank shouldn't upgrade their machines. They can reduce the points of vulnerability [for the customer] but they can't take it down to zero."

Fortifying an ATM to defend against skimming attacks ranges from the simple to the complex. For instance, a simple step is installing a PIN-pad guard that blocks the user's hand from view during PIN input.

Users are becoming savvier about protecting themselves at the ATM. Most people know that if a stranger is standing too close to the ATM, it could be a thief trying to steal their PIN.

More complex approaches include a variety of technologies that greatly reduce the risk of data loss to skimming. However, no security is 100 percent foolproof. Also, ATM operators may make the investments but feel that it may compromise the security to promote the upgrades to their consumers.

"It's not a cheap solution, and one of the things that scares people away is knowing that the investment in adding anti-skimming features won't totally stop the problem," said Nautilus Hyosung America's Bruno.

A number of ATM manufacturers, Nautilus Hyosung and Diebold among them, have adopted the CPK + 6000 series anti-skimming product range from TMD Security as upgrades for legacy machines. The CPK — short for Card

Protection Kit — incorporates a variety of technologies to make skimming very difficult, if not impossible, for criminals. TMD Security designed and produced custom solutions in close cooperation with ATM manufacturers, enabling seamless integration of the CPK in the machine.

Available for motorized and non-motorized or dip card readers, the CPK uses radio frequencies to create a protection shield around the card entry slot, which disables any device placed on the card reader. That way, the ATM can remain in service, but the skimming attack is denied.

"The device from TMD is one of the very few security measures that is available for any model of ATM regardless of manufacturer," said McKay. "If an ATM operator has an installed base with a range of different models and manufacturers, the TMD unit is the only one that could be introduced across the base."

The CPK is triggered by the Surface Detection Kit (SDK), which detects any foreign device placed over the card entry slot. The SDK can detect a variety of materials, including plastic, paper, iron and wood. Once activated, the CPK can send an alarm to an alarm panel. It also will track the number of skimming attacks at that location.

The full anti-skimming package also includes TMD's Tilt and Vibration Kit (TVK). This kit is designed to prevent criminals from attaching a skimming device in direct contact with the prehead/main reading head of the card reader inside the ATM. The TVK detects any attempt to cut or drill the ATM fascia to attach a skimming device. The TVK is invisible from the outside of the device and will fit any ATM or self-service terminal.

TMD's anti-skimming technology has been implemented successfully by banks and financial institutions worldwide, and it is offered by most of the major ATM manufacturers and value-added resellers.

"We have proven, the last five years, that something can be done about skimming," said Cees Heuker of Hoek, chief executive officer of TMD Security.

In 2007, Bankenes Standardiseringskontor, the national standards organization for the banking industry in Norway, implemented new standards for anti-skimming in the wake of numerous attacks. BSK reviewed a variety of approaches, but "we found the best solution for Norway was offered by TMD Security," said Geir Bonde, a senior consultant for BSK.

All ATMs in Norway are equipped with

Criminals use small cameras aimed at a PIN pad to detect a user's PIN. That number is then used to create false credit/debit cards and make transactions or is sold to another criminal organization.

TMD's CPK solution. Now Norwegians are safe from skimming attacks while at home. However, the financial industry has to remind Norwegians traveling abroad to be careful of skimming attacks because the attacks are no longer an issue at home.

"Norwegians don't think about skimming. I know I don't," Bonde said.

Manufacturers of ATMs are including anti-skimming measures in their new designs. For instance, Diebold Inc.'s Opteva line includes an award-winning technology that can recognize a skimmer placed on an ATM card reader.

"It uses a proprietary algorithm along with a sensor to detect skimmers of basically any size or shape or material," said Terrie Ipson, marketing manager for ATM security solutions for Diebold, a Canton, Ohio-based services company providing integrated technology solutions that enable customers to maximize their self-service and security capabilities.

Once a skimmer is detected, security systems also can send an alert. Depending on the system, the alert can be sent to a monitoring center, to a branch alarm or to dispatch local law enforcement. "What the financial institution wants to do with the alert is up to them," Ipson said.

The Opteva and the Personas line from NCR also include a feature called jittering. Rather than smoothly accepting the card, the machine's intake feature starts and stops in a rapid combination sequence, or a jitter. Any magnetic-stripe information that is copied at the card reader is useless because of the back-and-forth motion.

Duluth, Ga.-based NCR, a provider of assisted- and self-service solutions, upgraded 1,200 ATMs at HDFC in India with jitter-enabled card readers.

Jittering alone is no longer sufficient to protect the ATM. Criminals are circumventing jittering by using the DSP. Also, when a customer removes his card from a terminal, the action is typically done in a smooth motion, without jittering, enabling criminals to copy data from the magstripe. Jittering also does not protect swipe-card and dip-card readers.

Wincor Nixdorf, a leading provider of self-service equipment for financial institutions, takes a common approach to stopping skimming by taking the machine out of service if an attack is detected. Many of its machines have a plastic anti-skimming insert in the cardreader slot. The insert is designed to prevent tampering but does not restrict usage by customers.

If the insert is destroyed or the machine is moved by force, the machine is taken out of service immediately. If so equipped, video monitoring can be engaged to survey the situation.

Remote monitoring

Skimming detection and protection are only part of the security equation. For a complete solution, monitoring and alerts are necessary for a full defense against skimming attacks.

Remote monitoring software is designed to monitor and send alerts about the status of an individual ATM and the network as a whole. The software transforms this

information into alarms and follow-up actions to give operators control of the situation.

Managing a fleet of ATMs without a remote monitoring solution requires much greater physical interaction with the network and machines at a much higher cost. Such a network also is much more vulnerable to security breaches. Expensive service calls are much more common, and machines may be out of service more often due to common problems such as paper outages, device error and/or software hang-ups.

With remote monitoring, an ATM operator can minimize the number of times someone has to go out and physically touch the machine. When a technician is dispatched, there's a much greater likelihood he will have correct components and materials to fix the problem he is going to encounter at the ATM. Otherwise, a technician wouldn't necessarily know why a unit was out of service, and what parts might be needed to return it to service, causing delays and more downtime for the ATM.

Continuous flow of real-time data from remote monitoring enhances security for an ATM network. Recurring notification of a card reader failure or a drastic decline in transactions at an otherwise high-traffic ATM might be an indication of tampering. Other types of failures could indicate sophisticated software attacks.

In 2009, TMD launched its Premium Protection Service to protect and monitor the CPK + 6000 kits in ATMs 24 hours a day, seven days a week.

Continuous flow of real-time data from remote monitoring enhances security for an ATM network.

The solution includes the CPK+ equipment as well as monitoring infrastructure. The monitoring of IP video cameras is integrated with the trigger information provided by the CPK + 6000. The solution enables remote device management with live video information from a central place in the bank's network.

TMD has announced a partnership with ATM deployer Diebold to offer TMD products and remote monitoring to its customers.

"As a trusted partner and leader in providing ATM security solutions, Diebold is committed to working with our financial-institution partners to help reduce financial losses and maintain confidence in the ATM channel as a whole," said Chuck Somers, vice president, ATM security and systems, Diebold, when the partnership with that company was announced.

Enabled by the communication among the CPK, SDK, TVK and ATK components, TMD is able to monitor all the ATM security measures and other critical transactional parts. The regular service provider from the bank will perform first-line maintenance and can manage secure uploading of software upgrades. TMD will provide second- and third-line support to the service provider and manufacturers,

and will continuously evaluate new types of skimming attacks to increase the protection offered by the CPK + 6000 kits.

It's a way for ATM operators to have a turnkey solution to skimming protection.

"Fraud attempts by criminals, service or staff employees are countered with unique intelligent status monitoring of critical system parts. The PCK7 communication kit from TMD Security makes it possible to monitor the protection of the ATM without interfering with the existing software stack and communication protocol on the ATM. The great advantage is that we are able to connect a total ATM network, independent of brand, model or age of the ATM," said Heuker of Hoek.

Chapter 3 ATM software security

Like any other businessperson, leaders of the skimming gangs are interested in efficiency. Their desire is to steal as much money with as little cost as possible. Skimming data from individual ATMs can be a time-consuming and risky proposition.

Attacking ATMs via software can automate the process on a much larger scale.

Software also can play a defensive role, enabling efficient monitoring and response to attacks on behalf of ATM owners and operators.

ATM manufacturers have to increasingly guard against insider attacks. Criminal organizations may bribe lower-level technicians for access to machines, or even have members of the gang secure employment with a bank or service company to access the ATM network.

Cyber criminals collaborate in the online world, perhaps never meeting one another in person. The attacks are increasingly sophisticated, and always relentless.

For instance, criminals in Russia recently targeted ATMs with malicious software. The manufacturer responded quickly with a security upgrade.

ATM operators increase their exposure to these kinds of hacks with a few simple shortcuts, such as using compromised administrative passwords, not using the locked-down version of Windows that the manufacturer provides or failing to properly configure the firewall software. Experts reported this particular virus required an insider's knowledge of ATM operations, and access to the machines to install because it did not self-propagate like other viruses. However, the manufacturer announced that there was no insider involvement in the software scam.

NCR guards against insider threats with its Solidcore for APTRA, a software security solution that prohibits the introduction of unauthorized code into an ATM. The solution is a "white list," in that only authorized code is allowed to run on the

How criminals can gain access to an ATM network

- **Bribery.** Criminal organizations may pay lower-level technicians for access to machines.
- **An inside job.** A member of a criminal gang could gain employment at a bank or service company.
- **Collaboration.** The online world can bring criminals together, increasing their ability to breach security measures.

Criminals increasingly are turning to software to increase the efficiency and effectiveness of skimming attacks.

machine.

The accepted code cannot be modified, deleted or hijacked. That stops the replicating feature of viruses in which malicious code replaces authorized code with itself.

The underlying operating system can leave an ATM vulnerable as well. Many machines still operate on older versions of the Windows platform that have known security flaws.

"Manufacturers keep the ATMs simple to keep the price down, but keeping it simple also means it's fairly easy for the criminals," said ATMIA's McKay.

Another line of defense is to design the internal structure of the ATM so that it restricts access to the computer hardware inside. For instance, NCR's family of SelfServ ATMs utilizes a protected USB architecture that is self-contained within the ATM, helping mitigate the risk of fraudulent connection of unauthorized USB devices to the ATM.

ATM software plays a significant role in monitoring for skimming attacks and sending alerts when necessary. Of course, there's a fine line between a high level of security and a rash of false alarms due to oversensitivity to conditions.

Video monitoring

Video monitoring can help reduce costs and downtime associated with false alarms. If an anti-skimming device sends an alert regarding a suspected attack, a video monitor can ensure a speedy response without a physical inspection. If it truly is a false alarm, the ATM can remain in service, or be returned to service, and maintain availability for customers.

"You don't want to generate a lot of false alarms, and video monitoring helps because then you have the ability to actually see if there is something going on," said Diebold's Ipson. "There's always a balance between maintaining security and having false alarms."

When Diebold developed its monitoring software, one of the goals was to ensure accuracy.

If an anti-skimming device sends an alert regarding a suspected attack, a video monitor can ensure a speedy response without a physical inspection.

"We wanted to make sure those algorithms and sensitivities were set in a way that didn't generate false alarms," Ipson said.

Diebold is experimenting with video analytic technology, Ipson says. The software analyzes the video image of the ATM fascia, searching for any object that doesn't match the reference photo.

"It can search for an object left behind on the ATM and then send an alarm to the monitoring center, where they can look at the video to see if there was a skimmer placed," Ipson said.

Wincor Nixdorf's ProView security software responds to threats in a variety of ways. In addition to traditional remote monitoring, it's also integrated with anti-

skimming modules. If the sensors detect suspicious activity, the system sends an event or alert via ProView.

The system can activate a camera and photograph the perpetrator, take the ATM offline and generate reports. If the camera is disabled, it can take the machine offline as well. The software can restore the machine to operating status when the incident is investigated.

Predictive software

For years, credit card companies have used predictive software that monitors customer spending patterns. The software looks for purchases that are being shipped to an address other than where the monthly bill goes. It analyzes the orders, scanning for large purchases of electronics, jewelry or other easily sold goods.

Similarly, banks in the United Kingdom have started using predictive software for ATM/debit cards. McKay says the criminals are predictable when they prepare to withdraw money, using information from skimmed cards.

"Sometime before midnight they'll do a balance inquiry to see how much they can get, and withdraw money shortly before and after midnight," he said.

Midnight is typically when the daily withdrawal limits are reset. With information on the criminal's behavior, banks have started randomly changing the daily withdrawal limit reset time.

McKay says with coordination from the banks and LINK, the U.K.'s switching organization, police recently have been able to nab some skimmers.

Gartner's Litan supports the use of the back-office pattern-detection software to catch fraud. She believes it's a more effective — and cost-effective — solution than upgrading thousands of individual ATMs and point-of-sale terminals.

"It's not perfect, but it could take the fraud down to manageable levels," she said.

Chapter 4 User security

Ultimately, skimming attacks undermine customer confidence in the banking system. The blow to customer confidence may be a larger cost than the actual cash losses. However, the financial industry has been reluctant to raise awareness in a large-scale fashion in many countries. Certainly, customer protection agencies, law enforcement and even some financial institutions try to raise customer awareness about protecting card data.

However, some in the industry think more should be done.

ATMIA's Lee believes customers should receive more education about protecting their PINs by covering the hand used to key in the PIN at the ATM, to help prevent illegal PIN capture.

"This simple measure alone would significantly reduce the success rate of skimming attacks," Lee said.

But raising the awareness of skimming attacks could impair customer confidence in the ATM networks. Because of that, many financial institutions don't communicate to their customers all the security measures that are in place.

"Banks can't advertise what they've done because it could send a sense of uncertainty to their customers," said Nautilus Hyosung America's Bruno.

Defense against skimming begins with the basics of ATM placement that help the users and deter criminals.

Customers need to take precautions when using an ATM. ATMs in busy, well-lit areas are more likely to have security measures in place.

"Look at the environment itself, making sure there's good lighting, and security and surveillance around the installation," said Diebold's Ipson.

In Boca Raton, Fla., local police officers partnered with ADT Security Services to educate customers about skimming. ADT had installed anti-skimming devices on ATMs at some local banks, but declined to specify which ones for security reasons. The ATMIA noted that Florida is the second-worst state in the United States for ATM crime.

Raising the awareness of skimming attacks could impair customer confidence in the ATM networks. Because of that, many financial institutions don't communicate to their customers all the security measures that are in place.

The increasing sophistication of skimming devices increases the importance of guarding the PIN. Because it may be all but impossible to determine whether a skimming device has been attached, it's likely a customer could unwittingly give up the card data.

Protecting the PIN

Some anti-skimming measures are designed into new ATMs, and they should be invisible to end users. Passive approaches, such as PIN-pad shielding, are becoming more commonplace.

For instance, Diebold's Opteva ATMs incorporate a recessed fascia design so that the consumer blocks the PIN pad while entering the code. Diebold offers a PIN-pad shield for current and legacy machines.

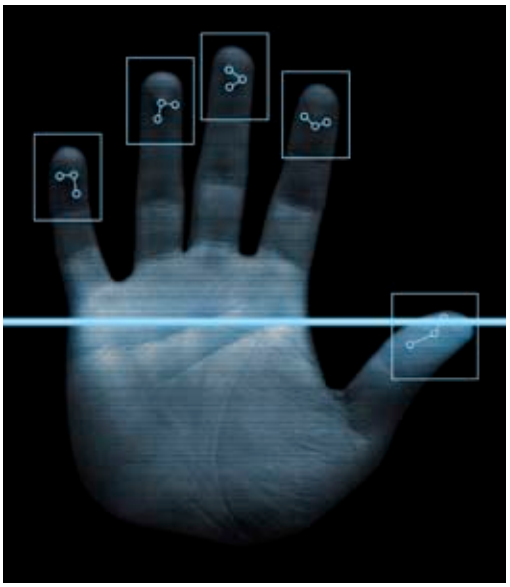
In Europe, a campaign to educate consumers to guard their PINs has paid off. ATMIA's McKay believes helping customers guard the code perhaps is the most effective way to fight fraud. He compares the PIN to the key to the front door of a person's home. The magnetic-stripe data is similar to the home address.

"If somebody knows my address, that's fine, but they don't have the key to the front door," McKay said. "We have to educate consumers that their PIN is their front door key, so don't give it away."

The increasing sophistication of skimming devices increases the importance of guarding the PIN. Because it may be all but impossible to determine whether a skimming device has been attached, it's likely a customer could unwittingly give up the card data.

"The average person would not know the skimmer is there," McKay said. "That's why it's so important the PIN is protected."

PIN-pad shields also can be retrofitted to legacy machines. Australia Technology Management introduced the PINGuard to block PIN theft attempts. The PINGuard is a polarizing lens or vision-control system arched over the PIN pad. The user has a clear view of the pad to enter the numbers, but from other angles the shield is opaque. This device shields the PIN from both surreptitious video surveillance as well as shoulder surfing.



Biometrics, the reading of fingerprints, retina patterns and other measurements of the human body, are the next frontier in ATM security.

Some skimming defenses are basic but effective in reminding users to think about security. Many ATMs incorporate small mirrors so that users can see if someone is standing behind them, shoulder surfing for the PIN. Even if no one is there, the mirror is a good reminder to take precautions.

Some manufacturers are designing visual cues into the fascia that indicate to users whether a skimming device has been placed over the card reader.

NCR calls its solution a Fraudulent Device Inhibitor. It's an illuminated hardware feature, or kit, that makes it difficult for criminals to attach foreign devices on or around an NCR ATM card reader. Diebold offers a similar solution, with LED lights around the card reader.

Customers should be aware of the feature and what it means.

"If the consumer doesn't see the lights, it would be one indication there's a skimmer in place," Ipson said.

Diebold has stepped forward to raise awareness for customers, developing a website promoting secure ATM usage.

"We promote awareness with consumers to inspect the machine before they use it, and shield their PIN," Ipson said.

Biometrics — the use of fingerprints, retina patterns and other measurements of the human body — are the next frontier of ATM security. It's another level of authentication that could supplant the EMV chip currently gaining widespread use.

Chapter 5 EMV technology

Banking systems in countries around the world are turning to EMV technology to increase their defenses against criminal organizations. EMV uses a computer chip embedded in the card to hold cardholder data. The chip replaces the vulnerable magnetic stripe. It takes its name from Europay, MasterCard and Visa, the three card brands that originally supported its development.

It has been implemented in the United Kingdom and has been mandated for Canada with rolling deadlines throughout much of the rest of the world. For instance, the Single Euro Payments Area initiative has mandated that EMV be implemented by 2010.

However, like other well-intentioned mandates, there have been unforeseen consequences. Although the incidence of ATM fraud has dropped dramatically in countries that have implemented EMV, fraud has migrated elsewhere.

The European Payments Council cautions that countries without EMV remain at significant risk of criminals using stolen card data to withdraw cash. Countries that have adopted EMV take a belt-and-suspenders approach to the magnetic stripe.

"Card issuers want an international card, so most chip-equipped cards still contain a magnetic stripe with cardholder data," said ATMIA's McKay.

That still leaves card information vulnerable.

"Unless all countries move to chip and PIN and there's no more mag stripe, the crooks can still commit a lot of crime," said Gartner's Litan.

Some countries implementing EMV

- Argentina
- Australia
- Brazil
- Canada
- China
- France
- Israel
- Mexico
- South Africa
- Turkey
- United Kingdom

The United Kingdom is seen as an effective test case for EMV, as conversion is estimated at well over 90 percent.

Financial Fraud Action UK, formerly known as APACS, reported that payment-card fraud committed by criminals using stolen U.K. card details in countries yet to upgrade to chip and PIN has nearly doubled in two years.

The organization noted, however, that while card fraud losses increased, losses as a percentage of plastic card turnover amounted to 0.1 percent in the first half of 2009 — equating to around a tenth of a

Although the incidence of ATM fraud has dropped dramatically in countries that have implemented EMV, fraud has migrated elsewhere.

penny lost to fraud for every £1 spent on cards — less than the 0.14 percent in 2004.

Counterfeit fraud losses fell by 48 percent for the first half of 2009, compared with an increase of 18 percent in 2008 and a 46 percent rise in 2007.

Financial Fraud Action UK notes that the vast majority of this fraud is due to criminals stealing card details in the United Kingdom to make counterfeit magnetic-stripe cards for use in countries yet to upgrade to chip and PIN.

Europe has led the way with EMV adoption, with almost complete implementation in the United Kingdom. France also has made great strides. Turkey has taken the opportunity to add smartcard applications as well as enhance security with the chip technology.

More than 20 countries in Asia-Pacific are implementing the technology, with China and Australia launching major projects. In the Middle East/Africa region, major markets lead the way as well, such as Israel and South Africa. Brazil, Mexico and Argentina are pursuing EMV conversion in Latin America. There, the largely unbanked lower-income segments of the population can store transaction details and other personal information on the card, making it easier to track purchases for marketing research.

The United States is still the largest holdout to the EMV trend, despite adoption by Canada and Mexico on its borders. Industry experts estimate the cost to convert the payments infrastructure to EMV at more than $10 billion, a less-than-compelling business case given the level of fraud and the economic climate.

The major ATM and self-service manufacturers have integrated EMV capability in order to sell units in countries that have adopted the standard. But a wholesale, coordinated conversion in the United States seems unlikely without some form of mandate.

“Not every bank will adopt the chip and PIN, and so there will be magnetic stripe on the card, and criminals still will be able to grab data from the mag stripe,” said Nautilus Hyosung America’s Bruno. “A mandate would move the United States in that direction, but I don’t think it will be a solution that can be implemented in one year or even five years.”

Conclusion

The ATM industry is locked in an arms race with organized, technologically adept criminal syndicates with tentacles that reach literally around the world. But is it a war that can be won?

Unfortunately, the industrious criminals have turned their efforts to cracking the chip technology. Relying on card technology alone to guard data may ultimately be a losing proposition for the industry that leaves ATMs otherwise unprotected against skimming.

Denying skimmers continuing sources of new card information can help slow the spread of fraud, so protective technology at the ATM is still a valuable weapon in the anti-fraud arsenal.

Denying skimmers continuing sources of new card information can help slow the spread of fraud, so protective technology at the ATM is still a valuable weapon in the anti-fraud arsenal.

However, a holistic approach seems to be the most effective.

"There are no silver bullets," said Gartner's Litan. "You have to take a multilayered approach, you have to protect the data from getting stolen in the first place, and use fraud detection systems to stop the use of the card information."