The payment card industry is coping with strong forces of change on many fronts. Not the least of these is the shifting terrain of fraud attacks. In recent years, attention has focused on massive breaches of cardholder data occurring through retailers and other institutions. While this kind of crime continues, we’re now seeing an abrupt rise in the incidence of card compromises resulting from attacks on bank ATMs.

The alacrity with which fraudsters modify their targets and methods underscores the need for the industry to fight fraud in a manner that is both comprehensive and flexible. Continued vigilance in basic measures addressing known vulnerabilities must go hand-in-hand with constant adaptation to emerging and changing threats.

This white paper:

- Presents data from the FICO® Card Alert Service showing the rapid rise of PIN card compromises at bank ATMs from 2008 to 2010.
- Discusses changes in ATM technologies and fraud methods contributing to this growing threat.
- Highlights key countermeasures banks with ATMs should be taking now, including proactive steps to minimize risk of cards being compromised as well as reactive strategies, after an attack, to minimize opportunities for fraudulent use of compromised cards.

Identify compromised cards faster and adapt quickly to changing fraud patterns with the maximum protection provided by FICO® Card Alert Service and FICO® Falcon® Fraud Manager
To some degree, the trend indicates a shift in fraudster focus. Figure 2 is based on statistics provided by the DataLossDB.org and Open Security Foundation. It shows that large-scale card compromises and data breaches, which dominated press headlines and reached their peak in 2008, have diminished.
This downward trend may reflect the fact that increasing awareness of these crimes—touching off loud public and legislative outcries—has caused companies handling payment card and cardholder data to install standards-compliant, point-of-sale (POS) equipment and/or adopt more secure database management practices. It’s also likely that all the press coverage made this type of opportunity too “hot” for many criminals. Bank ATMs began to look relatively more attractive, being out of the spotlight and, in many cases, under-protected.

While the number of cards compromised per bank ATM incident is generally a fraction of the numbers involved in incidents of institutional database hacking, the damage to card issuers can nevertheless be quite severe. Cardholders often react very negatively when the point of compromise (POC) is their bank, since they expect and trust financial services providers to keep their accounts and sensitive data secure. Moreover, demand deposit and current accounts may be a hub for other accounts and service relationships. Compromised cards and PINs are highly valued by fraudsters as potential gateways to multiple sources of funds. The overall sense of violation for the customer and aggregate losses for the bank can be substantial.

Why are bank ATMs vulnerable to renewed attention from fraudsters? One reason is that the devices and methods fraudsters use to skim card data and capture PINs have become increasingly sophisticated, efficient and, in some cases, less risky for perpetrators. Another reason is that some banks have not evolved their security to keep up with network-based threats to newer ATM technology. At the same time, the FICO Card Alert Service continues to see plenty of POCs where bank ATMs were left open to attack because basic security best practices hadn’t been followed or had been inconsistently applied.

To bring down the rising rate of bank ATM card compromises, financial institutions must implement all best practices for proactive defense—from basic measures to the latest recommendations. In addition, they must ensure that when a compromise does occur, they’re able to act quickly and efficiently to minimize the potential for damage. By “efficiently” we mean actions that, on the one hand, reduce the chances at-risk cards will be used to withdraw funds or make purchases, and, on the other hand, keep the impact on customers and cost to the issuer as low as possible.

Fortunately, in the wake of large-scale data breaches, many banks have already adopted more efficient methods of managing card compromises. Rather than indiscriminately blocking and reissuing cards, they now have the means to differentiate compromised cards by degree of risk and, therefore, to take a risk-appropriate action for each card. These methods should be used for all card compromises, regardless of the POC.

The rest of this paper examines these bank ATM vulnerabilities and the proactive best practices banks can use to minimize the risk. We’ll also look at best practices for isolating and containing the damage when card compromises do occur, as well as how new technology-based banking services, such as mobile transaction notifications and inquiries, are strengthening defenses by enabling cardholders to participate in fraud detection.
Here are the major developments in bank ATM fraud observed via the FICO® Card Alert Service, that analyzes the daily transactions of over 11,000 financial institutions.

**1. ATM card skimming methods are harder to spot, less risky for criminals, more risky for banks**

**Equipment**
- Criminals now identically match skimmer paint color to the ATM manufacturer’s façade, making discovery more difficult.
- Super glue and magnets are becoming the preferred methods for attaching skimmers to ATMs, as they are less visible than double-sided foam tape and more durable under a wide range of temperatures.
- Skimmers may be designed to take advantage of the built-in features of the host ATM (e.g., openings around card acceptor areas allow flashing lights to shine through).

**Installation/retrieval**
- Skimmers are often placed on ATMs Saturday mornings, then removed on Sundays before the financial institution reopens for business on Monday.
- Once installed, skimming devices are usually kept under observation. If the device is discovered, fraudsters will try to remove it fast before law enforcement arrives; if traffic is low, they may move it to a different location.
- Skimming devices with a USB port are being used more frequently, allowing criminals to return to the device and download data at any time.
- MP3 storage devices are commonly re-engineered to create skimming devices that provide larger storage and wireless capabilities.
- With wireless technology becoming ever smaller and more reliable, transmitters are easily hidden inside fake PIN pads and card readers, as well as within brochure holders and hollow ATM ceilings. Using the wireless connection, fraudsters parked in nearby vehicles may download card and PIN data after each transaction, sometimes sending the booty immediately across the internet to remote partners. Time and date stamps for both card and PIN data make it easy to match up the right data for counterfeit cards.

**Dissemination/usage**
- The time delay from skimming to unauthorized withdrawals and purchases has decreased from an average of 30 days in 1999 to mere hours in 2010. Often, card and PIN data is harvested in one country and quickly sold in another country or continent.
- Compromised cards with pending expiration dates are often first to be used for a withdrawal or purchase, as fraudsters seek to extract as much value as possible while the card is still good. By prioritizing cards for usage in this way, fraudsters maximize the return on their skimming investment.
- Bank Identification Numbers (BINS) may be sorted for sale to other criminals wanting to exploit the cards of a specific financial brand. Criminals may even attempt to perform “us on us” withdrawals (e.g., using a Bank of America card at a Bank of America ATM) to make their activities look normal and avoid detection.
Card Compromises—New Risks and Best Practices

Improve your ATM defenses:

- **Adopt corporate visual standards.** Every ATM should look exactly the same so that deviations in appearance will be easier to spot.

- **Make it obvious that security inspections are frequent and timing is variable.** Signage should clearly convey that the bank is actively managing ATM fraud risk in a manner that is not predictable by fraudsters.

- **Concentrate inspections during high-risk periods.** After-hours, particularly weekends and holidays, are prime time for skimmer installation.

- **Leverage inspection knowledge.** Use branch or security vendor personnel experienced at performing ATM security inspections. When this is not possible, incorporate expert knowledge into tools. For example, an approved photograph of the ATM in its proper state—with annotations showing areas warranting particular attention—will help a less-experienced inspector perform an effective visual comparison.

Figure 3: Increasing sophistication of ATM skimming devices

Sophisticated skimming devices such as this one are harder to spot since they are designed to allow features of the host ATM, such as flashing lights, show through the attached equipment.

2. Traditional surveillance methods are easily evaded by savvy fraudsters

- Criminals know how to prevent standard factory-installed ATM cameras from recording their activities. Common tactics include wearing hooded sweatshirts, sunglasses and baseball caps while positioning the head to make it difficult for cameras to get a clear image. Alternatively, fraudsters may simply tape a sheet of paper over the camera lens.

- Factory-installed cameras can be disabled by vandalizing them with an ice pick or baseball bat. Generally, the ATM will continue to function even when the camera is not operating.

- While observing an ATM where a skimming device has been attached, or when wirelessly downloading card and PIN data from the device, fraudsters will take up a position where their activity and vehicle license plate are outside of the range or at the peripheral of cameras.
Card Compromises—New Risks and Best Practices

» INSIGHTS

Improve your ATM defenses:

• Immediately upgrade to a digital video recording (DVR) system. DVRs provide much higher image quality and storage capacity than VCR or analog surveillance equipment.

• Install cameras in multiple locations. Additional cameras should be placed in hard to reach areas like roof lines and landscaping so that significant events can be captured without accidentally compromising cardholder PINs. Cameras should be aimed at all points of access to the facility, and all parking lot entrances and exits.

• Maintain archive footage for one year or longer. Video from the recent past may be critical to a forensic investigation in the near future. Storage capacity and fast, easy retrieval are additional reasons for going digital.

Figure 4: Getting the picture

One of the most common failures in dealing with bank ATM attacks is a lack of adequate footage of the suspects and their vehicles—largely the result of relying on a single factory-installed ATM camera.

3. Hacking and other programmatic attacks on ATMs are increasing

• Modern ATMs, which are connected to the internet and to financial institution networks, are vulnerable to attacks via viruses, Trojan horses and other malware just like other networked computers.

• Actual attacks as well as well-publicized demonstrations at security conferences have shown that ATMs can be controlled and their firmware overwritten by a determined, talented hacker with a network connection or even a USB key. Cases in point include an ATM made to eject money like a slot machine, another made to debit five dollars for every twenty dollar withdrawal, and another made to record and send a history of users’ card and PIN numbers to the hacker.
Improve your ATM defenses:

• **Keep ATM software up-to-date.** Immediately verify that every ATM has updated security patches and continue to install updates as they are made available.

• **Run detection software by the book.** Perform regular full-system checks using software that detects Trojan horses, viruses and other attack software. Follow vendor guidelines for keeping security software scrupulously up-to-date.

• **Change passwords frequently.** Verify that all default maintenance and user passwords have been changed upon installation.

• **Lock ATMs securely.** Use the high-security locks recommended by industry experts. Consider using unique keys for unlocking and opening the outer housing of each unit rather than universal keys, which tend to be duplicated and can present an increased security risk.

• **Beware the unbalanced ATM.** If an ATM becomes inexplicably out of balance, have a digital forensics expert examine it. The machine may have developed its tilt from tampering during a malware installation.

4. There are still plenty of brute force incidents

• In this age of technologically sophisticated fraudsters, it may be surprising to realize that physical removal of the ATM unit from its foundation, so-called "ram raids," are still the second-largest threat to ATM security after physical card skimming.

• The methods used to remove ATMs from their foundations vary depending on how securely the machine has been installed.

• Once the thieves have the ATM, they take it to a clandestine location where they can break into it at their leisure.

Improve your ATM defenses:

• **Bolt it down.** All free-standing ATMs should be bolted to their foundation to deter theft.

• **Send out the alarm.** Outfit equipment with alarms triggered by substantial movement or removal.

• **Locate machines on the move.** Some ATM manufacturers now offer global positioning satellite technology (GPS) to aid in the location and recovery of stolen equipment.

The proactive best practices we’ve described will make a bank’s ATMs more difficult to attack and thus relatively less attractive to criminals than other potential targets. They will not make an ATM crime-proof. Here are additional measures all banks should take to ensure that when card compromise events do occur, they are able to initiate effective action without delay.

Taking the right actions when you suspect your bank ATM has been attacked

• **Secure and monitor the ATM area.** Do not leave the ATM unattended, which would provide fraudsters with the opportunity to remove the attached skimmer or other device. Cordon off the ATM using caution tape from a standard robbery kit. Assign a bank employee to stay at the site until law enforcement personnel arrive.

• **Observe the perimeter.** Cautiously note unusual persons or lingering automobiles that may be of interest to law enforcement.

• **Contact law enforcement immediately.** Have a prepared list of law enforcement contact numbers (apart from 911) so that you don't waste time.

• **Secure surveillance footage.** Have it ready for law enforcement personnel when they arrive.
Alert internal counteraction team. Banks should have a pre-identified leader, and at least one backup person. It’s also helpful to have an email distribution list covering everyone within the organization who needs to know about a potential compromise.

Visually examine the ATM. While waiting for law enforcement personnel to arrive, perform a detailed visual examination of the ATM and surrounding area. Do not touch the machine, but look for things that don’t belong on or near it (e.g., devices, sticky adhesive residue, unauthorized brochure holders, and unusual openings in the ceiling, floor or walls).

If a compromise is confirmed through video footage or a confiscated device, notify your ATM network and the FICO® Card Alert Service. FICO will perform analysis and identify, when possible, “at-risk” cards. The Card Alert Service will issue a Compromised Card Report (CCR) alerting affected issuers to the compromise and a list of their at-risk cards will be provided within the CCR.

Receiving alerts about attacks on other ATMs as well as POS skimming and data breaches

Find out before compromises result in large losses. There’s often a considerable delay before card issuers are notified of POCs occurring at other ATMs on networks they’re not a part of or at retail points of service (POS). In addition, it often takes weeks or months for the results of forensic investigations of large-scale database breaches to be made available. Instead of waiting, card issuers may attempt to act on preliminary information, but because it’s so imprecise, they’re likely to over- or under-react, causing unnecessary costs, customer impact and losses. Subscribers to the FICO® Card Alert Service, however, receive far more timely and precise information about a wide range of card compromise events and threats. (See the sidebar “Two-fisted fraud defense.”)

Managing at-risk cards

Take appropriate actions based on predictable risk. Many card issuers struggle with how to handle cards that have been exposed to some form of data theft. The card associations as well as FICO Card Alert Service generate millions of cards each year earmarked as “at-risk.” While this classification indicates that a card has a higher than normal probability of risk associated with it, it does not mean that the card will inevitably be used for a fraudulent withdrawal or purchase. Blocking and reissuing every at-risk card is an unsustainable practice from the point of view of both cost ($3.50 to $30 per reissue) and impact on cardholders. Issuers should take actions appropriate to the actual risk level for each at-risk card.

Establish an at-risk policy. To guide their decisions regarding at-risk cards, issuers should determine what rate of fraud (ROF) is considered to be excessive by their standards for acceptable loss. For example, an issuer might decide to perform a blanket block-and-reissue for all at-risk cards appearing on a single compromised card report when the fraud percentage rate for that group of cards reaches 10% or more. When the ROF is below that threshold, the issuer would apply more selective treatments, as described in the next three bullets.

Block and reissue high-risk cards. Consider reissuing cards approaching their expiration dates, since these will often be used first by fraudsters. Reissue is also recommended for high-net-worth accounts and customers with multiple accounts and/or service relationships that represent high aggregate value. Prioritizing these accounts, and providing personalized attention and service during the reissue process, reduces the risk of large fraud losses and of customer attrition.
INSIGHTS

- **Monitor all other at-risk cards.** All at-risk cards not blocked and reissued should be “hot carded”—entered into an analytics-based transactional fraud detection system so they can be monitored for future fraud activity and swift action taken if it occurs. Monitoring can also be used as an interim treatment when issuers have extremely large batches of cards identified for block and reissue, and require time to complete the task.

- **Review or automatically deny transactions on some monitored cards.** Cards with risk that is not high enough for immediate block and reissue, but is still higher than most of the other cards being monitored can be targeted for transaction interception. A series of real-time denials on cards from a particular issuer can quickly discourage criminals from using cards issued by that institution. The best fraud detection systems enable nontechnical personnel in fraud management to quickly write/modify business rules to apply different levels of scrutiny and adjust review/denial thresholds for specific groups of at-risk cards.

Bring Customers into the Fraud Detection Loop

Increasing account transparency and access, so that customers can efficiently monitor their own accounts for unauthorized transactions, is a “force multiplier.” It greatly expands the number of eyes watching for unusual activity, improving the chances of minimizing fraud in the wake of a card compromise. Most issuers are focusing such initiatives on mobile and other online channels—opportunities to not only reduce fraud but increase brand strength and customer stickiness. Still, some measures can be implemented through simple enhancements to traditional monthly printed statements as well.

**Incoming communications**

- **Make all balance inquiries visible.** Because balance inquiries generally have no monetary value (no fee is debited from the customer’s account for performing the transaction), consumers rarely see them reflected on their monthly statements or during online banking sessions. But criminals regularly perform balance inquiries to test PINs. If accountholders have the opportunity to see all such activity, nonmonetary or not, they may question some transactions and quickly alert their financial institution.

Two-fisted fraud defense

For maximum fraud defenses—both proactive and reactive—rely on these fully integrated FICO solutions:

**FICO® Card Alert Service** detects potential fraud and identifies points of compromise (POCs) and at-risk cards for ATM/payment processing networks and their participants. Using a patented Accelerated Detection process, the service analyzes daily ATM transaction volumes across nearly 11,000 financial institutions to spot suspicious activity. It then works with issuers to validate the fraudulent transactions before researching cardholder transactional histories to identify a common point of compromise (ATM, point-of-sale, organizational database), where criminals may have gained access to cardholder data and PINs. By analyzing transactions at those locations, the service identifies cards likely to have been compromised during the time window during which the attack occurred, then provides issuers with reports on these at-risk cards.

**FICO® Falcon® Fraud Manager** is the most accurate and comprehensive solution for detecting payment card fraud across multiple types of accounts. Reducing losses by up to 50%, it is relied on by 17 of the top 20 credit card issuers worldwide. The new release, FICO Falcon 6, includes cutting-edge analytics that adapt detection to changing fraud patterns and cardholder behavior in the production environment, enabling you to detect up to 44% more fraud. It’s the best way for issuers to closely monitor at-risk cards, assign risk-appropriate levels of scrutiny and, if suspicious activity occurs, take rapid, efficient action to prevent large losses.
• **Provide an up-to-date record of telephone banking activity.** Online and monthly statements should include brief details on all accounts accessed during telephone banking sessions so that unauthorized account access can be quickly identified by the customer.

• **Keep customers informed of card hold status.** Customers should be able to review information about all payment card holds when they log in online or initiate telephone banking sessions. In this way, potentially fraudulent transactions can be identified before they are posted to the account.

**Outgoing communications**

• **Deliver daily balance updates.** Send customers their current account balances using their preferred method of communication (customer-designated email account, SMS, etc.). Abrupt changes in balance will alert the customer to a potential issue.

• **Enable customers to establish alert thresholds.** Offer alerts for ATM withdrawals over a customer-set limit, for “out of area” transactions beyond a customer-specified distance from home or place of work, for card not present (CNP) transactions, for deposit activity, etc. Customers receiving an alert to an unfamiliar transaction are likely to alert their financial institution immediately.

**Conclusion**

Today bank ATMs are a target of renewed interest to fraudsters. Financial institutions that fail to improve their defenses against rising attacks are likely to suffer the highest losses.

Next year, or even sooner, a new fraud trend will emerge. To meet emerging threats, fraud management solutions must be both comprehensive and highly adaptive. They must be proactive to minimize risk of card compromises and reactive to minimize risk that compromised cards will be used. In this constantly shifting fraud terrain, all industry participants need to be ready to cover more ground.

Improve your defenses against bank ATM attacks and other emerging fraud threats:

• Join the Card Alert Fraud Forum website, where over 6,000 members network and share incidence of fraud on a daily basis: www.fraudalertnetwork.com. Membership is free for all financial institutions and law enforcement officers. Website registration required.

• Sign up to participate in FICO’s ATM Photo Resource Directory project (one contact per institution). This annual directory of financial institution contacts who administer ATM image requests is available only to participating financial institutions. Law enforcement agencies may request a complimentary copy without participating. For more information, please email JohnBuzzard@fico.com.

• For assistance with any ATM skimming situation, call the FICO® Card Alert Service Team directly at +1 888 440 4227, Monday through Friday, 9:00 AM EST to 6:00 PM EST.

• Network with other fraud professionals and discuss the latest fraud trends by attending FICO’s free monthly webinar series: “Combatting fraud through peer communication.”