

ATM FRAUD AND SECURITY



**Minimizing loss, mitigating risk
and maintaining consumer
confidence in the ATM channel.**

Introduction

According to estimates by Retail Banking Research, there are over 1.5 million ATMs installed worldwide, with new ATMs being installed approximately every 5 minutes. Millions of successful ATM transactions are carried out each day, and the ATM has been used safely for more than three decades. Even so – like most devices designed to secure and dispense items of value – they are susceptible targets of fraud.

It's easy to overestimate the scale of ATM fraud. ATM thefts, burglaries, and electronic fraud make great headlines, and it seems national and local media rarely miss a chance to sound an alarm with regard to ATM attacks. After all, who could resist a story about two guys, a pick-up truck, a chain, and an ATM — especially when those two guys always seem to leave their license plates behind at the scene of the crime! >>



We won't rest.

It's important to note, though, that most of what the media call "ATM Fraud" is actually Debit Card fraud – having much more to do with the compromise of Personal Identification Numbers (PINs) and fraudulent Debit Card use than with the integrity of ATM hardware systems.

In fact, the Global ATM Security Alliance reports that just .0016 percent of all ATM transactions are affected by crime or fraud, worldwide.

Notwithstanding this record of secure transactions, ATM fraud and security have emerged as leading topics of interest among owners and operators of ATMs. Minimizing losses, mitigating risks, and maintaining consumer confidence in the ATM channel are logical priorities for financial institutions and others who deploy ATMs.

This white paper contains a comprehensive overview of ATM fraud, security, and consumer safety issues facing the self-service industry. It describes fraud techniques and introduces management practices and devices designed to keep ATMs secure.



Global Trends

In April of 2006, Russian police arrested a group of criminals accused of stealing at least \$500,000 from US bank accounts in a cross border ATM scam. The gang obtained stolen account information and PINs from organized crime groups in the U.S., Canada, and France to make fraudulent cash withdrawals at ATMs in Moscow. The funds were stolen from the accounts of U.S. citizens who had never been to Russia.

This case, like so many others, highlights the increasingly global nature of ATM fraud. Criminals and victims are often on different continents, and the problems of one region become the problems of another. Here's a look at geographical trends associated with ATM fraud.

Europe

Card skimming was the biggest crime affecting ATMs in Europe in the past year according to a survey of 325,000 ATMs in 27 European countries by the European ATM Security Team. Card skimming at ATMs caused losses of nearly EUR 44 million across Europe, and is a source of funding for Eastern European organized crime.

The good news is that the number of skimming attacks has dropped by 20 percent since 2004, and related losses are down by 43 percent. These drops are likely related to Europe's implementation of anti-fraud devices – plus the migration of more than 50 percent of European ATM card readers away from magnetic stripe cards to more secure EMV chip cards. In fact, France is benefiting from its nine-year transition to chip cards, where ATM fraud is down by nearly 80%.

The bad news is that cash trapping and transaction reversal crimes are on the rise, especially in Eastern Europe, as criminals look for other ways to steal money. In these cases, thieves fix a device to the cash-dispensing slot, causing notes to get stuck inside. The criminals return to remove the cash from inside the dispenser. Trapping attacks resulted in reported losses of EUR 2 million in 2005.

Latin America

Latin America is one of the fastest growing ATM markets in the world – with deployment booming in Brazil, according to Frost & Sullivan Research. Many countries in the region, such as Argentina, are deploying highly advanced ATMs, where customers can trade stocks and manage their personal finances.

Unfortunately, excessive fraud and corruption are hampering many financial institutions' growth plans. ATM card fraud rose in Latin America by nearly 15 percent in the past 5 years.

In response, the region is accelerating anti-fraud measures, especially with the use of EMV chip cards. Brazil leads this migration effort, where card fraud has recently fallen by more than 80 percent. However, smaller markets, such as Chile and Peru, are facing a much slower transition.

Asia

China and India are also two of the fastest growing ATM markets. China now has over 86,000 machines in use, and the Indian ATM market is growing at a rate of 100 percent year-on-year, according to Frost & Sullivan Research. And, due to the lower Internet adoption rate in some regions of Asia, Web-based ATMs are filling the void for online banking.

But as financial institutions rapidly expand their Asian ATM base, they're also seeing an increase in crime. The top ATM fraud in Asia is dispenser trapping.

Asia is also the origin of much of the world's phishing attacks – although the victims are often on other continents. In these scams, "spoofed" e-mails, that appear to be coming from a bank, lead consumers to counterfeit web sites that trick them into giving their account information and PIN numbers. These fake web sites, that look identical to real bank web sites, are often hosted and routed through Chinese or Indian servers.

Criminals then use the stolen account information to create fake ATM cards and make withdrawals. Phishing attacks have been increasing over the past year, according to a recent Gartner study.

North America

North America is the largest ATM market in the world. Canada leads the world in per-consumer transaction volumes, while the US has the largest installed base. But the widespread use of ATMs – with over 14 billion cash withdrawals in the US alone – makes North America an attractive target for criminals around the globe.

Physical attacks against ATMs are popular in North America. Criminals attempt to remove the machine from its location, often by tying a chain to it and detaching it with a truck. Once they succeed, they use mechanical tools, torches, and explosives to open the safe door or make an opening in the safe walls.

In the US, ATM card-related fraud has risen sharply. In August 2005, Gartner estimated that about 3 million US consumers had been affected by ATM card fraud in the previous year – with annual losses of \$2.75 billion, or \$900 per incident. And these amounts exclude secondary losses, such as negative publicity for the financial institution and lost consumer confidence.

ATM card fraud in the US is expected to increase dramatically in the coming years. A major factor is the

fact that the transition to EMV chip cards is happening throughout Europe, Asia, Latin America, and Canada – but not the US. Chip-based cards are much more difficult to counterfeit than magnetic stripe cards, which are relatively cheap and easy to duplicate. As organized criminal groups become discouraged by other countries' antifraud measures, they are likely to view the US as an increasingly attractive target.

A Global Problem

ATM Fraud is happening on a global scale. As the world comes closer together, a bank customer in Australia may have a run-in with a criminal in Bulgaria. And a scheme that works in France today may end up in Canada tomorrow.

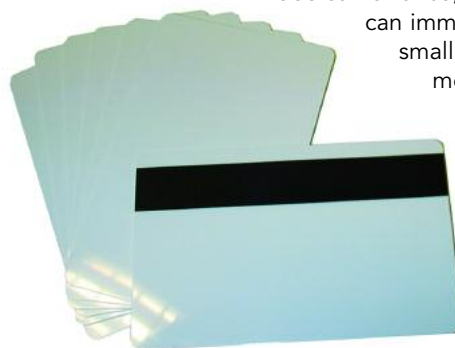
With this in mind, the ATM industry must take a global view of ATM fraud by tracking crimes against ATMs in every part of the world and developing solutions to prevent their evolution.

Types of ATM Fraud

Card Fraud

Given the intense focus manufacturers are placing on security-related engineering of ATMs, it's not surprising that the most vulnerable component of any ATM system can't be found on an ATM. Instead, it can be found in the pockets, purses, and wallets of ATM customers. It's the ATM card. And once compromised, the data it contains can lead to many of the most common types of ATM fraud.

Armed with a customer's Personal Identification Number (PIN) – often obtained through casual observation – a thief with data from a magnetic stripe can reproduce or clone ATM cards using inexpensive, commercially available equipment. And by taking precautions to hide or obscure his or her identity from video surveillance, such a fraudster can immediately steal small amounts of money or easily empty a customer's bank account within a matter of days.



Operational Fraud

Bank fraud can also occur when ATMs are accidentally or purposely stocked with currency in the wrong denomination – thereby giving customers or criminals more money than should be dispensed.

As recently as September, 2006, WAVY-TV reported an incident in Virginia Beach, VA, where a hacker unlawfully obtained administrative privileges for a gas station's freestanding ATM. The hacker used this ill-gotten data to reprogram the ATM to operate as if it were loaded with \$5.00 U.S. bills instead of \$20.00 U.S. bills – enabling himself and many other customers to walk away with four times the money requested for withdrawal.

This fraud was made possible when factory-installed default passwords were left in place on an ATM configured to allow ATM administration through a consumer-accessible interface. Apparently, the thief learned his trade by downloading an online copy of the ATM's technical programming manual.

Equipment Fraud

Another concern for operators of ATMs is fraud related to fake ATM equipment. This ranges from add-on devices such as fake card readers or skimmers to ruses involving false fascias or even bogus ATMs.

The first recorded instance of using fake ATMs dates all the way back to 1993, when a criminal gang known as the Buckland Boys installed a fake ATM at a shopping mall in Manchester, CT. Like most fake equipment, it



On-screen warning concerning potential fraud.

was not designed to steal money. Instead, the fake ATM appeared to customers as if it did not work – all the while stealing card data from everyone who attempted to use it.

Digital Fraud

The migration from proprietary operating systems to Microsoft Windows® technology has led to greater connectivity and interconnectivity of ATMs. Vast networks – including ATMs, branch systems, phone systems, ticketing systems, and other infrastructure connected via the World Wide Web – are susceptible to a new kind of threat, a threat to digital security.

Digital attackers include vandals who author viruses or worms intended to exploit an ATM's operating system and criminal hackers attempting to violate the confidentiality, integrity, or authenticity of transaction-related data.

Types of ATM Security

Digital Security

ATM digital security systems should be designed to prevent intrusion, defy hackers, and stop digital crime before it begins. ATM security experts recommend a strong firewall featuring multiple layers of security. An important first step is to lock down, or "harden," the ATM. This means making all electronic points of entry invisible or unavailable to hackers, viruses, and worms. This technique is made possible through a combination of a strong firewall and software designed to monitor, analyze, and authenticate any external source attempting to connect to an ATM. This solution should be designed to block any unauthorized user or pattern of data.

In fact, a good digital security system should be able to analyze and compare patterns of data to those of known attacks and send alerts upon detecting suspicious activity.

Patch management is another important component of any digital security system. From time to time, Microsoft releases security patches – security-related updates to its operating system – designed to eliminate known problems with its operating system. ATM digital security systems should be designed to identify appropriate patches and to quickly deploy them throughout an ATM network in an effort to protect against viruses, worms, and other digital exploitation.

Physical Security

Since their invention, ATMs have been designed to resist physical attacks. Yet that hasn't completely stopped concerns over physical security.

Many physical attacks are designed to steal the entire ATM and to transport it to a location where its safe can be laboriously penetrated and its contents removed. Other methods of attack, such as ram raiding, are simply brute force attacks designed to effectively demolish ATMs and steal cash. Since the late 1990s, for example, organized groups of criminals in Japan have improved ram-raiding techniques by using heavyweight trucks or heavy construction equipment to uproot and destroy ATMs before removing their contents.

Another physical attack method is to seal every opening of an ATM with silicone before filling the vault with combustible or explosive gas. In this manner, ATMs have been compromised when explosions from within have distorted or opened their vaults sufficiently for removing their contents.

As a result, more modern approaches to physical security, including the use of ink dye systems designed to render currency useless, have gained in popularity as a mechanism for deterring physical attacks.



Vandalized ATM in Spain

Transactional Integrity & Security

The security of ATM transactions relies not only upon the level of secrecy employed by individual ATM users, but also upon the secure operation of encrypted, trusted microprocessors.

Most countries have laws requiring data encryption at ATMs. In the U.S., sensitive data at ATMs was traditionally encrypted using a Data Encryption Standard (DES) or information processing standard mandates by the federal government. Today, however, DES is considered by most cryptographers to be insufficient for protecting ATM transactional data, and a new standard known as Triple DES has emerged.

With each new wave of electronic crime perpetrated on ATMs, their operators, and their users, manufacturers of ATMs must increase research, development, and engineering efforts aimed at guaranteeing the security and integrity of ATM transactions.

Device Operation & Security

In most countries, financial institutions are liable when ATM systems fail. This simple fact suggests ATM owners and operators need to take great care to secure and ensure proper functionality of ATMs.

With this in mind, modern ATM engineering has resulted in improved fascia design, weather and vandal-resistant construction materials, shutters, and other devices designed to protect and ensure the integrity of ATM components.



Customer Identity Security

While ATM operators are certainly concerned with protecting the identity, account information, and personal data of their customers, it's important to note that identity theft cannot be committed through ATMs.

There is insufficient personal information available to fraudsters during breaches of ATM security to commit offenses such as setting up false bank accounts or attempting to "prove" a false, personal identity.

Consumer Safety at the ATM

An April 2006 poll by Harris Interactive found that 37 percent of adults who have a bank account are more concerned than they used to be about using ATMs for



In an effort to provide increased safety and to minimize shoulder surfing, some financial institutions have indicated privacy areas by painting or otherwise marking the floor beneath their ATMs.

reasons relating to security. Not surprisingly, then, consumer safety has become a leading consideration in the manufacture, deployment, and management of ATM networks.

Manufacturers have experimented with mirrors, better lighting, emergency call buttons, video surveillance, and other devices intended to provide a more secure environment surrounding ATMs. Financial institutions are more carefully evaluating ATM locations, more often stressing the importance of consumer awareness, and have gone so far as to arrange for security patrols at high crime, high traffic locations.

ATM Fraud Techniques

Card Theft

Beyond obvious approaches such as mugging or stealing from mailboxes, criminals use a variety of techniques aimed at stealing ATM cards. Most of these attempts involve a technique known to security experts as “card trapping.”

Card trapping involves placing a device directly over or into an ATM’s card reader slot. Such devices are designed to retain cards after customers insert them. Often, a “helpful” thief will then suggest a customer re-enter his or her PIN in an effort to attempt the card’s return – of course, to no avail.

Later, after the unsuspecting customer has departed, the thief can remove the trapping device or fish out

the card. Then, by entering the PIN that the thief has just observed, the thief can access and withdraw funds from the customer’s account.



A Lebanese Loop

One variant of this approach is to trap the card inside the ATM’s card reader with a device often referred to as a Lebanese Loop. When a customer walks away, frustrated by not getting the card back, the criminal is able to remove the card and withdraw cash from the customer’s account.

This method is often combined with the “droplet” method of stealing a customer’s PIN. With this method, small drops of oil are placed on PIN pad keys. After a customer uses an ATM, the oil makes it obvious which keys have been pressed and easy to quickly discern the entered PIN.

Card Skimming

Another method of accessing a consumer’s account information is to skim the information off of the card.

Skimmers are devices used by crooks to capture data from the magnetic stripe on the back of an ATM card. These devices – smaller than a deck of cards and resembling a hand-held credit card scanner – are often fastened in close proximity to or over top of an ATM’s factory-installed card reader. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM card.



Card skimmers

An inexpensive, commercially-available skimmer can capture and retain the information from more than 200 ATM cards before being re-used. Such personal information includes account numbers, balances, and verification codes associated with each cardholder.

Typically, these devices are used to fool consumers into believing that the skimmers are part of the ATM

equipment. The boldest of thieves have gone so far as to place signs on ATMs instructing cardholders to “swipe here first” before continuing with transactions. Another fraudulent method is to portray the additional card reader as a “card cleaner” designed to extend the life and improve the performance of ATM magnetic stripes.

Shoulder Surfing

Shoulder surfing is nothing more than the act of direct observation as a person taps onto an ATM PIN pad. Criminals typically position themselves close – but not in direct proximity – to legitimate ATM customers and watch covertly as the customer enters his or her PIN.



Miniature Video Camera records PIN entry

A more sophisticated take on shoulder surfing is accomplished through the installation and use of miniature video cameras aimed to record PIN entry.

Fake PIN Pad Overlays & Other Fake Equipment

This criminal technique involves the placement of a fake PIN pad directly over top of an ATM's original PIN pad.

This overlay captures and stores PIN data with each transaction. The fake PIN pad is later removed, recorded PINs are downloaded, and the information is combined with counterfeit ATM cards to obtain funds illegally from legitimate customer accounts.



fake PIN pad records PIN entry

Fake PIN pads are often identical in appearance and size to original equipment. Furthermore, they are often razor thin or transparent, making detection nearly impossible for consumers. With these types of PIN pad overlays, transactions actually proceed in a normal way.

Criminals also attach portable monitors and card readers to ATMs. Fake card readers and PIN pads record the requisite information for illegal withdrawals while fake monitors provide bogus screens explaining that transactions cannot be completed.

PIN Interception

This high-tech approach to stealing PIN information results from the capture of data through an electronic data recorder. This is possible from within the ATM terminal or as PIN data is transmitted for online verification. Either approach requires access to the inside of an ATM; therefore, this type of crime is often perpetrated by organized “professionals” at off-premises ATM locations.

Accessing Cash with False Presenters

This fraud is performed through the addition of bill traps or false presenters in front of ATM dispensers. These traps are placed over to disguise the normal dispensing operation of the ATM.

During the course of an otherwise normal transaction, an ATM will dispense notes into the trap; however, those notes are never presented to the customer. Assuming the ATM has malfunctioned, the customer leaves. After that, the criminal returns, removes the bill trap or false presenter, and leaves with cash that was intended for the customer.

The simplest form of bill trap involves the placement of adhesive tape in a manner which blocks the cash dispenser, holds delivered banknotes, and prevents cash retraction. A more sophisticated approach employs a motorized device designed to deliver banknotes into a dedicated, hidden bin, thus simulating a more natural, “real” withdrawal of banknotes.

Another method begins with a legitimate cash withdrawal transaction – possibly with a stolen card. In this method, the criminal does not take the note stack when presented. Instead, the criminal allows the notes to retract after a certain period of time – as if they were forgotten. For a brief period of time, those notes sit in the ATM's presenter before being diverted into a “retain” bin. By prying open the presenter door and grabbing the retracted notes at exactly the right time, criminals can obtain the cash, but the transaction is still reversed and no funds are debited to the account associated with the “legitimate” transaction.

Transaction Reversal

Transaction reversal scams use a variety of methods to create an error condition at the ATM that result in a transaction reversal by the host processor due to the reported inability to dispense cash. Meanwhile, the cash has been taken through accessibility or force.

Here's an example. An ATM user requests a withdraw of \$100; however, when the note stack is presented, the user carefully removes only a portion of the banknotes in the stack. A few moments later, the transaction times out and the remaining notes are returned to the ATM. Since the ATM cannot count how many banknotes are retracted, it will often (depending upon host software and bank policies) reverse the entire transaction – leaving the user with some of the cash withdrawn but with no corresponding debit.

Burglaries

Physical attacks are sometimes attempted on safes inside of ATMs, through mechanical or thermal means. The goal of these attacks is to penetrate the ATM to open the safe door or to make an opening sufficient to remove cash.

Operational Fraud

Operational fraud, typically, is perpetrated from within. Employees responsible for ATM management can accidentally expose ATMs to fraud by making sensitive information readily available to fraudsters. Or worse, employees with unfettered access to ATMs and related customer information can use that access to commit crimes that are difficult to detect.

Fighting Fraud & Securing the ATM

Video Surveillance

The primary method used to increase awareness and deter fraud attempts at the ATM is the installation of Closed Circuit Television Cameras mounted in plain view on or near the ATM.

Nowhere does this sort of digital security offer more benefit than in the surveillance of off-premises ATMs, which present obvious challenges with regard to maintenance and security.

Cameras can be easily integrated into the fascia of most ATM machines, and improved security can be achieved by installing additional site cameras on and around the premises.

The availability of remote video surveillance services makes digital video an even more attractive security option, because many ATMs and their surrounding areas can be directly monitored from a single, central location.



Place video surveillance equipment near ATM.

Remote Monitoring

Remote diagnostic services provide an automated means to monitor and manage ATM networks. Remote monitoring can communicate important messages that may indicate tampering with a machine.

Remote diagnostics, monitoring, and management provide improved uptime and reduced risk. These services promote dispatch avoidance and enable a group of central support associates to control keyboard and mouse operations of ATMs directly from remote PCs.

Through ATM monitoring capabilities, status messages from an ATM can be sent to a central location where those messages are acted upon based upon a pre-defined plan. Central support associates can quickly identify problems and security concerns based upon the messages they receive. For example, the continual notification of a card reader failure or a drastic decline in transactions at an otherwise busy location might be an indication of tampering.



Remote management centers keep things going from a central location.

Remote diagnostic services also contribute to the safety and security of personnel assigned to work on ATMs, by giving these associates remote access and the ability to manage events from a secure location.

Preventing Card Theft

Card readers with the capability to detect if an ATM's card reader shutter is closed completely can provide an indication that a fishing device may have been inserted into the card reader. By using remote diagnostics to monitor the ATM, error codes generated by the card reader can be tracked. An increase in the occurrence of error codes related to card readers could be an indication that a fraud attempt is in progress.

Preventing Card Skimming

There are a variety of methods that may be employed to deter card skimming. To begin with, awareness among consumers, branch personnel, and ATM service technicians can result in the detection of devices added to an ATM fascia. Visual clues such as tape residue near

or on a card reader may indicate the former presence of a skimming device.

In addition, the following anti-skimming solutions can be introduced.

- **Jittering.** Jittering is a process that controls and varies the speed of movement of a card as it's swiped through a card reader, making it difficult – if not impossible – to read card data by the external device.
- **Alert systems.** These systems monitor routine patterns of withdrawals and notify operators or financial institutions in the event of suspicious activity.
- **Chip-based cards.** These cards house data on microchips instead of magnetic stripes, making data more difficult to steal and cards more difficult to reproduce.
- **Foreign object detection.** ATMs equipped with this type of technology can alert owners, operators, or law enforcement in the event that a skimming device is added on the fascia of an ATM.

Preventing Shoulder Surfing

Consumer awareness mirrors are the most effective method for deterring or detecting shoulder surfing. In addition, mirrors can be affixed to the fascia of an ATM, allowing users to easily see behind them as they enter data. Furthermore, PIN pad shields can be used to obscure data entry.

The ergonomic design of an ATM can also play an important role in preventing shoulder surfing. Techniques such as positioning the keyboard in the center of the fascia or recessing the display more deeply within the terminal can also make shoulder surfing more difficult.

Preventing Fake Equipment

Consumer education and ATM monitoring services are the best ways to prevent the application of fake equipment on or near legitimate ATMs.

Consumers should be taught awareness of the look and location of ATM components, such as PIN pads, card readers, monitors, and dispensers.

ATM monitoring services are designed to notify owners of repetitive time out messages during PIN entry.

Foreign object detection technology can also play a

role in identifying fake equipment. Hidden from view, this type of technology actively monitors the ATM's fascia. When abnormalities are detected, ATMs can notify authorities and even shut down until problems are resolved.

Preventing PIN Interception

Encrypted PIN pad technology is the key to preventing PIN interception. Encrypted PIN pads "scramble" data before transmission so that no raw PIN numbers are accessible to electronic hackers.

Preventing Transaction Reversals

Many financial institutions deter this fraud by always debiting the account for the full amount of a transaction, dealing with legitimate short-dispense claims as they arise. Other techniques include monitoring "time out on withdrawal" error messages. If this message occurs repeatedly and is associated with a specific cardholder, this may be an indication of criminal activity.

Finally, using a retract bin with separate compartments – each dedicated to a single retract operation – can allow financial institutions to associate specific, retracted banknotes with specific transactions.

Preventing Burglaries

There are a variety of mechanical and physical factors than can inhibit attacks to ATM safes. The certification level of a safe, for example, can determine how difficult a safe is to penetrate. A certification level of UL291 Level 1 is recommended as a minimum for ATMs placed in unsecured, unmonitored locations."

Alarms and sensors also reduce exposure to risks.

Further, the best defense against potential litigation by crime victims is a proven track record of policies aimed at crime prevention. Following are practices to consider for educating consumers, deterring crimes, and improving the security of ATM premises.

Consumer Education

- Make safety and security educational materials available.
- Provide safety information directly on ATM screens.
- Print safety and security reminders on ATM receipts.

Crime Prevention

- Videotape customers and ATM transactions.
- Provide video surveillance of parking lots and other areas surrounding ATMs
- Provide an emergency call button or telephone at ATMs.
- Document requests to local police to patrol areas surrounding ATMs.
- Increase security measures in areas of frequent crime.
- Use contracted security guards as patrols or as sentinels.
- Maintain records relating to security complaints; document action taken as a result of each complaint.
- Maintain record of proper security equipment maintenance.

Premises Protection

- Locate ATMs in highly visible, well-traveled areas.
- Employ high-intensity lighting at and around ATMs.
- Designate parking spaces dedicated to "ATM Use Only".
- Keep trees, shrubs, and other greenery well-trimmed; remove other obstacles that may obscure the view of ATMs and the areas around them.

Preventing Operational Fraud

The best defense against operational fraud is to establish and follow rigorous internal policies and procedures that limit access to ATMs and related passwords by branch personnel. Consider offering rewards for information regarding criminal activity, and ensure that bank employees know the consequences of operational fraud.

The Virginia Beach incident, described above, could have been prevented with good procedures in place, such as changing default passwords on every new ATM, or even avoiding the purchase of any ATM configured to allow administration through a consumer-accessible interface.

To ensure the highest level of protection against operational fraud, Fair Isaac CardAlert services recommends the following practices:

- Immediately verify that every ATM operated by your financial institutions has security codes that are not original manufacturer default settings. Leaving factory default settings is very common; however, it is an unsafe practice.

- ATM safe combinations should also be changed from original manufacturer's settings.
- Consult ATM user guides to ensure optimum operating standards, since ATM equipment varies by manufacturer.
- Ensure that sub layers within ATM security settings have also been reset to unique passwords or access codes.
- Balance your ATMs daily or as frequently as possible.
- Reconcile settlement account deposits with actual ATM balances to identify possible irregularities.
- Increase security around all ATM equipment.
- Make sure all video equipment is working properly. Date your video surveillance tapes and keep them secure for 60 days when possible, in case you need to refer back to them.

Conclusion

Fraud attacks on ATM networks are a worldwide phenomenon, yet they are of particular concern in the U.S., where the market is larger, transaction volume greater, and the use of chip cards is not yet widespread.

In August 2005, Gartner estimated that about 3 million US consumers had been affected by ATM card fraud in the previous year - with annual losses of \$2.75 billion, or \$900 per incident. These amounts exclude secondary losses, such as negative publicity for the financial institution and lost consumer confidence.

ATM fraud is growing because it produces cash and is fairly low risk relative to other crimes. The necessary equipment for criminal activity is inexpensive, readily available, and expendable.

ATM fraud also lends itself to organized crime. The fraud is repeatable. It is profitable. And it is not likely to end.

Even so, consumer confidence in ATMs remains high, and industry efforts to combat fraud, increase consumer awareness, and promote ATM security seem to be outpacing the growth rate of criminal activity.

New technologies such as video surveillance, remote ATM management, and foreign object detection – combined with common sense management practices aimed at deterring crime – are providing manufacturers with an edge in the fight against fraud and keeping the self-service industry at least one step ahead of the criminals.

About Diebold

From the Great Chicago Fire of 1871 to the present day, Diebold has been protecting the assets of financial institutions around the world. Diebold continues to evolve, protecting each facet of the banking industry; from branches, vaults and tellers to advanced self service terminals.

As the industry's leading integrator of security products, Diebold understands better than anyone what the financial industry's service and security support needs are now and will be in the future. Diebold is the premier company in the world that can provide enhanced security for ATMs.

Diebold's prominence in the financial security business for over 100 years allows our customers to depend on Diebold to provide solutions and recommended approaches to contain such issues as ATM fraud. Diebold boasts a world-class service organization with professional ATM service technicians that are trained to be cognizant of the new ATM fraud techniques and to conduct a detailed evaluation of key ATM components to ensure there has been no tampering or additions to the fascia.

We Won't Rest until our customers' customer feels secure throughout their ATM experience!



While Diebold has tried to be complete in the preparation of this material, it must be recognized that the criminal community too is ever expanding its knowledge and methods of defeating security features. Accordingly, the use or implementation of some or all of the methods described herein cannot be considered to be a guarantee that the security of any ATM cannot be compromised or that the security features in or around an ATM will operate continuously or error free at all times.

Call on Diebold to offer you the latest in product, service and security solutions.
Since 1859, Diebold has put its customers first.

Contact Information:
[Diebold, Incorporated](#)
Post Office Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

DIEBOLD[®]

We won't rest.