

ATM Fraud and Security

White Paper

Introduction

Over the past three decades consumers have come to depend on and trust the ATM to conveniently meet their banking needs. In recent years there has been a proliferation of ATM frauds across the globe.

Managing the risk associated with ATM fraud as well as diminishing its impact are important issues that face financial institutions as fraud techniques have become more advanced with increased occurrences.

The ATM is only one of many Electronic Funds Transfer (EFT) devices that are vulnerable to fraud attacks. Fraud against POS terminals for credit card authorization has been more prevalent as the account number can be used alone to begin charging against an account. Card theft, or the theft of card data, is the primary objective for potential thieves because the card contains all relevant account information needed to access an account. Card readers are one of the common peripherals used at both ATMS and POS devices. Although they utilize different mechanisms, their functions are the same; to read the data contained within the magnetic strip on the back of the card.

Fraud at the ATM, although more difficult than at a POS, has recently become more widespread. Recent occurrences of ATM fraud range from techniques such as shoulder surfing and card skimming to highly advanced techniques involving software tampering and/or hardware modifications to divert, or trap the dispensed currency.

Recent Global ATM consumer research indicates that one of

the most important issues for consumers when using an ATM was personal safety and security*. As financial institutions use the migration of cash transactions to self service terminals as a primary method of increasing branch efficiencies, the ATM experience must be as safe and accommodating as possible for consumers.

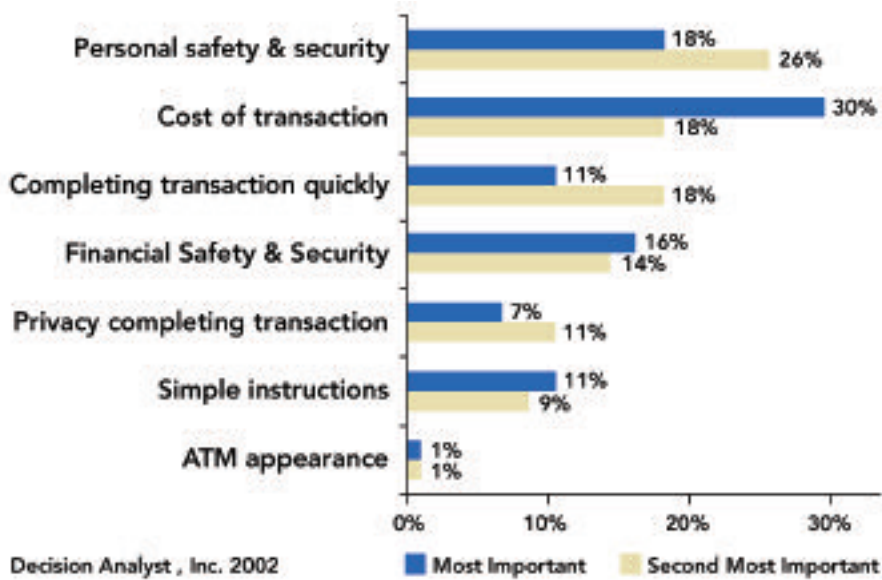
There are a multitude of security issues that surround ATMs such as burglary, fraud, physical attack/brute force removal, vagrancy and vandalism. ATM manufacturers are constantly enhancing their product lines to discourage these types of potential criminal activities.

It is important for each discipline within the ATM industry to work closely together to communicate and share detected ATM fraud methods. Financial institutions, networks, host processors and ATM manufacturers sharing experiences and knowledge will help the industry reduce and control this type of crime more effectively. There are immediate methods that can be instituted to minimize the risks associated with ATM fraud.

CONTENTS

Introduction	1
General Practices to Deter Fraud	2
Video Surveillance	2
Awareness and Consumer Education	2
Remote Monitoring	2
ATM Fraud Techniques	3
Card Theft	3
Skimming Devices	3
PIN Security	4
Shoulder Surfing	4
Utilizing a Fake PIN Pad Overlay	5
PIN Interception	5
Accessing the Cash	6
Application of a false ATM presenter	6
Transaction Reversal	6
ATM Burglary Attacks	7
Preventing ATM Burglary Attacks	7
Locks and Closing Devices	7
Mechanical Locks	7
Electronic Locks	7
Alarms and Sensors	8
INK Dye	8
Conclusion	9

ATM Customer Priorities



General Practices to Deter Fraud

Video Surveillance

The primary method used to increase awareness and deter fraud attempts at the ATM, is the installation of Closed Circuit Television Camera(s) mounted in plain view on or near the ATM. Video surveillance used in the branch environment has proven itself invaluable as it continually assists in the deterrence and apprehension of bank robbers. Video surveillance is the primary method used to increase awareness and deter fraud attempts at the ATM as well. Cameras can be easily integrated into the fascia of most ATM machines and optimum security can be achieved by installing additional site cameras on and around the premises. Nowhere does digital offer more potential benefits than in the surveillance of off-premise ATMs. Not only is continuous surveillance a critical security issue, legislatively mandated in many states, but remote sites offer particular challenges with regard to maintenance that can be solved with digital video recorders. The availability of remote video surveillance makes this option even more effective as monitoring of the ATM and surrounding area can be directed from remote locations at any time.

Awareness and Consumer Education

Deterrence of potential fraud attempts can be achieved by a joint effort involving finan-

cial institutions, the consumer, and ATM manufacturer / service provider. Financial institutions should stress the importance of awareness at the ATM to their customers and promote vigilance in reporting any irregularities in the appearance and operation of the ATM. Many customers use the same ATMs in their daily or weekly banking routines. Habitually using the same ATMs provides for familiarization with the aesthetics of a unit. An attentive consumer that notices irregular objects or any attached notes suggesting unusual operating instructions should immediately report the discrepancy to the financial institution's 800 number located on the ATM.

Financial institutions should confirm that their branch personnel, ATM services providers, and cash handlers are trained to recognize the latest ATM fraud techniques. Service technicians should be trained to conduct a detailed evaluation of key ATM components at each visit to ensure there has been no tampering or additions to the ATM. They should also be particularly cognizant of evidence that may reveal the use of adhesive tape on or near operating points such as card readers, pin entry devices, and dispense points.

It should be recommended to customers to carefully review their monthly account statements or to use internet banking to monitor for any uncommon activity on their account.

Recent ATM fraud has consisted of criminal rings actually purchasing ATMs and placing them in the open market. The ATMs end up being a repository for stolen card data and PIN numbers. Some criminals go as far as to set up the terminal with network association and actually dispense cash so as not to cause suspicion. Others will have a screen pop up that notifies that the transaction could not be completed after the consumer has swiped their card and entered their PIN. Promoting to consumers to use recognized ATMs could protect them from using an ATM that has been compromised to capture PIN and card information

Remote Monitoring

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

Remote diagnostics, monitoring and management provides improved ATM terminal availability and reduces risk. It promotes dispatch avoidance of service technicians and enables a group of central support associates to control, from their own PCs, the keyboard and mouse operations of ATMs. Through ATM monitoring capabilities, the status messages from an ATM can be sent to a central location where those messages are acted upon based on a pre-defined plan. The central support associates can quickly identify the problem based on the statuses

they receive. By having this capability, central support associates can control the ATM as if they were local at the terminal. This solution provides complete remote access to the terminal which reduces the risk for service personnel working on an ATM.

Remote diagnostic services track and manage events at the ATM, route and document every action taken. For example, the continual notification of card reader failure or a drastic decline in transactions at an otherwise high traffic ATM might be an indication of tampering.

ATM Fraud Techniques

This document has been created to provide a comprehensive overview of the possible fraudulent activities that may be perpetrated against ATMs. This document will also discuss the different techniques and methodologies of known ATM fraud attempts on a global scale and investigates recommended approaches to prevent or deter these types of fraud.

Card Theft

In an effort to obtain actual cards, criminals have used a variety of card trapping devices (Figures 1 and 2) comprised of slim mechanical devices, often encased in a plastic transparent film, inserted into the card reader throat. Hooks are attached to the probes preventing the card from being returned to the consumer at the end of the transaction. When the ATM terminal user shows concern due to the captured card, the criminal, usually in close proximity of the ATM, will offer support, suggesting the user enter the PIN again, so that

he or she is able to view the entry and remember the PIN.

After the consumer leaves the area, believing their card to have been captured by the ATM, the criminal will then use a probe (fishing device) to extract the card. Having viewed the customer's PIN and now having the card in hand, the criminal can easily withdraw money from the unsuspecting user's account.

Preventing Card Theft

Card readers with the capability to detect if the 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 cards readers could be an indication that a fraud attempt is in progress.

Skimming Devices

Another method of accessing a consumer's account information is to skim the information off of the card. Skimming is the most frequently used method of illegally obtaining card track data. "Skimmers" are devices used by criminals to capture the data stored in the magnetic strip of the card. Reading and deciphering the information on the magnetic stripes of the card can be accomplished through the application of small card readers in close proximity to, or on top of, the actual card reader input slot, so it is able to read and record the information stored on the magnetic track of the card. The device is then removed, allowing the downloading of the recorded data.

Skimming devices can be smaller than a deck of cards and read the magnetized strips on bankcards the way credit card scanners or ATMs read card information (See Figure 3 and 4). They can capture and retain the information from more than 200 cards, including account numbers, balances and verification codes.

These types of "skimmers" can trick the consumer into believing that the device is part of the ATM equipment. Small skimming devices (approximately 1.0 inches wide, 1.0 inches long) have been prominently attached with a sign instructing cardholders to swipe cards through the additional reader



Figure 1



Figure 2



Figure 3



Figure 4

“for security purposes” before performing a transaction. Another known method is to portray the additional card reader as a card cleaner.

Prevent Skimming

There are a variety of methods that may be instituted to deter card skimming. As mentioned earlier the attentiveness of ATM consumers, branch personnel, or ATM service technician can create awareness of any added modules to the terminal fascia. Visual clues such as the presence of adhesive tape residue near or on the card reader may indicate that a skimming device has been used

In addition, the following “anti-skimming” solutions can be introduced:

- Controlling the speed of the movement of the card or intentional erratic movement of the card during card insertion and return by the motorized card reader will confuse most skimming devices and make it impossible for the card information to be read accurately. This “jitter” technique is being incorporated into some new card reader designs. A good example of this is when a tape recorder skips a beat or more, which makes the sound distorted and not recorded accurately.
- Installing an auto alert system to monitor the routine patterns of withdrawals to help determine fraudulent withdrawals. There are risk management companies that provide early detection and common-purchase-point analysis of payment card fraud.
- Migration towards chip cards and chip card readers as the account information is housed on a chip rather than magnetic strips and is less susceptible to skimming (common outside of North America).

PIN Security

Once the criminal has retrieved the account information by either stealing the actual card or ascertaining the account information from a skimming device and replicating the information onto a counterfeit card, their next step is to get the Personal Identification Number (PIN). The PIN is one of the most important elements needed to steal the identity of an ATM user. The following techniques to acquire the PIN number must be

used in conjunction with methods used to apprehend the account information from the card in order to be useful to a criminal.

Capture of the Customer PIN may be attempted in one of the following ways:

- Shoulder Surfing (Direct Observation as the consumers enter their PIN number)
- Fake PIN Pad Overlay
- PIN Interception

Shoulder Surfing

Shoulder Surfing is the act of direct observation, watching what number that person taps onto the keypad. The criminal usually positions himself in close but not direct proximity to the ATM to covertly watch as the ATM user enters their PIN. Sometimes miniature video cameras (See Figure 5) that are easily obtained might be installed discretely on the fascia or somewhere close to the PIN Pad, to record the PIN entry information.



Figure 5

Preventing Shoulder Surfing

In addition to camera surveillance, a mirror can be affixed to the fascia of the ATM that would allow users to easily see behind them as they enter their information. Mirrors are an additional feature that should supplement the ATM being placed in a well-lit, open, high-traffic area.

The ergonomic design of the ATM plays an important part in preventing shoulder surfing as the positioning of the keyboard, centered directly below the monitor, allows for the body to naturally cover the area of pin entry. An ATM design that considers transaction privacy by recessing the display, and

positioning the PIN entry device in such a manner that will allow the consumer to easily block direct viewing of their transaction details by others, will deter shoulder surfing to a large degree.

Education of the ATM user is important to enhance their awareness of potential fraudulent activities or devices. With increased ATM usage requiring fewer visits to the branch, the ATM serves as a primary consumer interface, representing the financial institution. Illuminated signage panels, surrounding street lights and placing the ATM in a high-traffic area will provide a secure and welcoming environment to customers.

Utilizing a Fake PIN Pad Overlay

A fake PIN pad is placed over the original keypad (See Figure 6). This overlay captures the PIN data and stores the information into its memory. The fake PIN pad is then removed, and recorded PINs are down-

loaded. Fake PIN pads can be almost identical in appearance and size as the original. An additional type of overlay that is more difficult to detect is a 'thin' overlay that is transparent to the consumer. With this tool, not only is the PIN intercepted, it also allows for the transaction to proceed in a normal way. This method used in conjunction with card data theft provides the criminal with the information needed to access an unsuspecting consumer's account.

A criminal may also attach a portable monitor and card reader on top of the actual ATMs monitor and card reader to obtain the card and PIN information. The false monitor and card reader record the account information and present a message to the customer that the transaction cannot be completed; after the customer leaves the criminal will return and remove the portable device.

Preventing Fake PIN Pad Overlay

Educating ATM users to be aware of abnormalities in the look and feel of the keypad and paying attention to the screen as they enter their PIN is important in revealing fraud attempts. A warning that there might be a PIN pad overlay is no ***** asterisk appear on the screen when the PIN is entered.



Figure 6

Utilizing ATM monitoring software /services would enable notifications to be sent to the network if there are repetitive occurrences of a "time out message" during PIN entry. These messages could signify that a card has been inserted into the ATM, but the transaction has timed out because no data has been entered and the card returned, due to the pin pad overlay that has received the PIN entry information.

PIN Interception

After the PIN is entered, the information is captured in electronic format through an electronic data recorder. Capturing the PIN can be done either inside the terminal, or as the PIN is transmitted to the host computer for the on-line PIN check. In order to capture the PIN internally, the criminal would require access to the communication cable of the PIN pad inside the terminal, which can more easily be done, at off-premise locations.

Preventing PIN Interception

Electronic fraud continues to increase in both sophistication and loss exposure. To address this issue, MasterCard and VISA are requiring new PIN pad security enhancements for ATMs that tie into their network.

With normal keypads, the PIN number entered by the customer is sent in "raw" state via a cable to a separate circuit card module containing encryption integrated circuits. In order to decrease PIN theft fraud, VISA and MasterCard are now requiring an encrypted PIN Pad in place of the keypad. The EPP is a sealed module that immediately encrypts the PIN entry so that no "raw" PIN numbers are accessible to electronic hackers either tapping onto wires within the ATM or remotely sensing electromagnetic radiation emitted through ATM wiring. Any tampering of the EPP renders it unusable requiring shipment back to the manufacturer to reset internal keys.

In regards to on-line communication, the newly instituted Triple DES standard strengthens the encryption algorithm that is used to protect the secrecy of your Personal Identification Number (PIN) as it is sent from the ATM to your bank for verification.

Accessing the Cash

There are a variety of methods used by criminals to intercept, divert or otherwise illegally receive, dispensed currency.

- Application of a false ATM presenter to divert dispensed notes
- Transaction Reversal

Application of a false ATM presenter

This fraud is performed through the addition of traps in front of the dispense point. The device added to the terminal covers or disguises the normal dispense point. The ATM dispenses notes to the false front and are never presented to the customer. The customer mistakenly assumes the terminal has malfunctioned, and leaves. After the customer leaves, the criminal returns, removes the false front, and takes the currency. (See Figures 7, 8 and 9)



Figure 7



Figure 8

The simplest method is using adhesive tape that blocks the cash dispenser and holds the delivered banknotes, preventing note retraction. A more highly sophisticated method is using motorized devices that transport the delivered banknotes into dedicated bins internal to the device, thus simulating a real withdrawal of banknotes.



Figure 9

In Eastern Europe and South America, criminals were placing false black plastic covers over the presenter door with sticky tape on the inside. When the next legitimate customer attempted to perform a cash withdrawal transaction, the presenter would push the note stack against the sticky tape. Although the customer saw no activity, the ATM would

attempt to pull the notes back after the timeout period but some would remain held by the tape. The customer would leave assuming the ATM was not operating properly. The criminals would return a few minutes later to remove the fake cover and retrieve any note stuck to the tape.

Another method would begin with a legitimate cash withdrawal transaction (possibly with a stolen card) but the criminal does not take the note stack when presented. The notes would retract after a timeout period

but would sit in the presenter track momentarily before being dumped into the retain bin. By prying open the presenter door and grabbing some or all of the retracted notes within a small time window, the criminal would obtain cash but the transaction would still be reversed. No funds would be debited from the account.

Preventing application of a false ATM presenter

In order to reduce the likelihood of anyone successfully opening the presenter door and fishing out notes, the presenter door mechanics can be enhanced with a more robust locking mechanism. The firmware can also be modified so that the dump stack is moved further away from the presenter door while the push plate is moved forward directly behind the presenter door.

Another solution provides a modification to both the dispenser firmware and hardware. The firmware modification consists of a new dispenser memory PROM which changes the dispense and retract operation of the dispenser presenter. After the note stack reaches a certain position within the presenter, the final delivery of the note stack is done entirely by the belts without any assistance of the push plate. Should an external false cover with tape be present, there will be a much lower force pushing notes against the tape resulting in most or all of the notes being retracted.

Operationally, financial institutions should debit the customer's account whenever the dispenser sends a status message indicating that banknotes have been presented. If the dispenser performs a retract and dump, a transaction cancellation should only take place subject to an audit and verification.

Transaction Reversal

Transaction reversal scams use a variety of methods to create an error condition at the ATM which result in a transaction reversal by the host processor due to the reported inability to dispense cash, while the cash is legitimately accessible by force.

An ATM user may request to withdraw \$100. However, when the note stack is presented, they would only carefully remove a portion of the notes from the presenter mechanism. For example they remove \$60 from the center of the note stack – leaving \$40 in the presenter. Several seconds later, when the ATM times out and sends an error message to the bank, a “Time out on Withdrawal” occurs, and the ATM, depending on software application, retracts the banknotes left in the output slot, and deposits these banknotes into the retract bin of the dispenser.

The dispenser is not able to count how many banknotes are retracted, and usually (dependent on host application) the delivery amount is not debited to the Customer Account.

Preventing Transaction Reversals

The following preventative measures can be taken to avoid exorbitant financial losses:

- Many financial institutions deter this fraud by ALWAYS debiting the account for the full amount of the transaction, and dealing with actual short dispense claims as they occur. An individual that has attempted to defraud the institution will rarely do so by claiming a short dispense, as it will allow for scrutiny of transaction history and trends
- Monitoring the “Time out on Withdrawal” and resulting retract: if this error is recurring on a specific card, it may be an indication of fraudulent activity.
- Using a retract bin with separated compartments, each dedicated to a single retract operation, allowing the association of the retracted banknotes with the transaction.

ATM Burglary Attacks

Physical attacks are sometimes attempted on the safe inside the ATM, through mechanical or thermal means. The goal is to penetrate the ATM to open the safe door or to make an opening in the safe sufficiently large enough to remove the cash. There have been many highly publicized situations where criminals have actually physically removed an ATM from its location by tying a chain to it and driving off with the ATM dragging behind a pick up truck.

Preventing ATM Burglary Attacks

There are a variety of mechanical and physical factors that can inhibit attacks to the safe.

- The certification level of the safe (UL 291 Level 1 is recommended as a minimum for ATMs placed in unsecured, unmonitored locations)
- Alarms and sensors that will detect physical attacks on the safe
- Ink stain technologies that will ruin and make unusable any removed banknotes

Design, construction, and attack resistance ratings of safes vary according to local regulations. A certain level of robustness may indicate resistance, not only to the piercing of holes through the safe walls (with tools, torch, etc.), but also resistance to explosives, detachment from the floor to which the safe is anchored (again depending on local regulations and certification requirements). Depending on the class of the safe, either compliance to construction criteria (i.e.: UL) or to robustness criteria (CEN) minimizes a safes vulnerability to attack. Always insure that your ATM safes are manufactured, tested, and rated to security levels appropriate to the risk associated with the installation site.

Locks and Closing Devices

Mechanical Locks

ATMs today provide a range of solutions with different levels of security.

Mechanical locks allow the opening of the safe door only through the combination of different keys, whereby each key is in the hands of a different person (i.e.: two mechanical keys, one mechanical key and a combination lock, two combination lock).

Electronic Locks

Electronic locks provide an even higher level of functionality and convenience than mechanical locks. Electronic locks allow multiple combinations, each assigned to a different ATM maintenance facilitator, or different passwords for the operator, supervisor and conveyor (with different access rules)

Some electronic locks feature intelligence, i.e.: allowing the opening of the safe only during the specific time periods that have been pre-programmed. In addition, electronic

locks are able to report remotely (to a monitoring system) the open/closed state of the safe that must fit with a determined usage profile, otherwise this might indicate that a robbery is occurring.

Alarms and Sensors

Alarms are intended to:

- Detect the open/closed state of the safe door (also of the electronic cabinet of the ATM).
- Monitor different parameters that can be indicative of a robbery attempt.
- Report the status remotely to a monitoring center.

Sensors

Below is a list of the most common Sensors (able to detect different physical phenomena), together with the type of attack these alert.

Type	Alert Activity
Temperature	Piercing with torch
Tilting	Detachment of the safe (for transportation to other premises)
Vibration	Piercing with tools (drilling, cutting), wedging
Door	Door is tampered with outside of cash handling or servicing.

A smoke pump was instituted in Brazil to release smoke when an ATM was violated by a physical attack, like vibration or tilting. The smoke consumed the vestibule or lobby where the ATM was located to obscure the removal of the ATM. The sensor that released the smoke also sends notification to the monitoring center.



Figure 10

INK Dye

These systems consist of two base components:

- The Detectors
- The Ink Dyeing

Bank notes contained within the dispenser cassette are stained with ink when the control system detects an abnormality in the monitored parameters. Stained banknotes can no longer be circulated (See Figure 10), making the robbery attempt fruitless.

The dyeing of the banknotes can be triggered by an unauthorized attempt to open the safe (for these purpose security meshes, temperature, vibration, tilting sensors are used).

Conclusion

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.

To learn more about Diebold's ATM Fraud and Security Solutions, contact your Diebold sales representative.

Authored by: **Anna C. Istnick and Emilio Caligaris**
Product Marketing Managers,
Global Product Marketing and
Management Division of Diebold

Diebold, Incorporated
Post Office Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

DIEBOLD

We won't rest.

©Diebold, Incorporated 2003
All rights reserved. Litho in U.S.A.
10.03