RESEARCH PAPER | Commerce | Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Awareness of Atms in India

KEYWORDS

Mrs. P.Geetha

Ph.D., Research Scholar, Department of Commerce, Periyar University, Salem – 636 011.

ABSTRACT *ATM is one of the most popular means of cash delivery machine as it helps its customers to do Anywhere, Anytime banking. Though bankers and customers are gaining a lot, they are facing certain problems also. Hence, this study deals with the usage of ATMs, problems in ATMs, various types of frauds and techniques in ATMs, various measures and general practices to deter fraud and awareness about ATMs*

Introduction

Automated Teller Machines (ATMs) were the first well-known machines to provide electronic access to customers. With the advent of ATMs, banks are able to serve customers even after banking hours. ATM is designed to perform the most important function of a bank. It is operated by a plastic card which replaces cheque, customer's personal attendance, restrictions of banking timings and paper based verification. ATMs perform various banking functions such as withdrawal of cash, making balance inquiries, changing the PIN Number, depositing and transferring money from one account to another and register the mobile number. Though ATMs are rending valuable services to the customers, there are certain problems and threats regarding the usage of ATMs. How people should be aware of using ATMs are dealt in this study.

ATMs in India

India has approximately 79,000 ATMs as of June 2011. State Bank of India (SBI) is No.1 and has more than 25,444 ATMs. Axis Bank which comes No.2 with 6,871 ATMs and ICICI is No.3 with 6,425 ATMs. HDFC is in the No.4 position with 5,998 ATMs and PNB came No.5 with 5,375 ATMs. These 5 banks (SBI, AXIS, ICICI, HDFC and PNB) have almost 2/3 rd of all ATMs (63%: 53,000 out of 79,000 ATMs in India). Indian Banks together have an ATM network of nearly 1,00,000 machines dispensing cash across the country at the end of June-2012. This includes ATM at Banks as well as Non-Bank locations. SBI leads the pack with 22,469 ATMs, out of which 12,327ATMs were installed within the bank premises and 10,142Atms were installed outside the bank premises and it was followed by Axis Bank with 10,337 ATMs, out of which 2,096ATMs were installed inside the campus and 8,241ATMs were installed outside the campus. The difference between the First and Second is quite large for anyone else to come and fill the gap.

ATM Cards

India is one of the fastest growing countries in the plastic money segment. Already there are 130 million cards in circulation, which is likely to increase at a very fast pace due to rampant consumerism. India's card market has been recording a growth rate of 30% in the last 5 years. Card payments form an integral part of e-payments in India because customers make many payments on their card-paying their bills, transferring funds and shopping. Ever since Debit cards entered India, in 1998 they have been growing in number and today they consist of nearly 3/4th of the total number of cards in circulation. Debit cards usually allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash and as a check guarantee card.

Advantages of ATM Cards

Debit Cards plays a significant role in withdrawing cash at any where in the nook and corner of the world. A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can easily obtain a debit card, allowing him/her to make plastic transactions. Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks, thereby making personal checks merchants' transactions quicker and less intrusive. Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge other than a foreign ATM fee.

Problems of ATMs

Though ATMs are convenient in withdrawing cash , helpful for knowing the available balances, changing the PIN Number etc, customers face many practical problems such as card locking, long duration of ATM card delivering, insecurity, machine break downs, long time in cash dispensing, link failure, problems with respect to PIN change and machine running out of cash.

ATM Fraud and Security

ATMs are facing the following problems. They are Card Theft, Skimming Devices, PIN Security, Shoulder Surfing, Utilizing A Fake PIN Pad Overlay, PIN Interception, Accessing the Cash, Application of a false ATM Presenter, Transaction Reversal and ATM Burglary Attacks. 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. 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.

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

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.

ATM Fraud Techniques

This article provides a comprehensive overview of the possible fraudulent activities that may be perpetrated against ATMs. It 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 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 customers PIN and now having the card in hand, the criminal can easily withdraw money from the unsuspecting user's account.

Preventing Card Theft

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. Information can be captured and retained 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 "for security purposes" before performing a transaction. Another known method is to portray the additional card reader as a card cleaner.

Prevent Skimming

Different methods are there to deter card skimming. 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. For example, 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.

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. 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 that are easily obtained might be installed discretely on the fascia close to the PIN Pad, to record the PIN entry information.

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-lighted, 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 extent. Education of the ATM user is important to enhance their awareness of potential fraudulent activities. Illuminated signage panels, surrounding streets 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. This overlay captures the PIN data and stores the information into its memory. The fake PIN pad is then removed, and recorded PINs are downloaded. 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

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

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 asterisks appear on the screen when the PIN is entered. 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 online 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. MasterCard and VISA cards require 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.

Accessing the Cash
There are a variety of methods used by criminals to intercept, or otherwise illegally receive, dispensed currency. Application of a false ATM presenter to divert dispensed notes, and 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, they 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. 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.

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 back away from the presenter door while the push plate is moved forward directly behind the presenter door.

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 or by force. An ATM user may request to withdraw Rs.10,000. 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 Rs.6,000 from the center of the note stack — leaving Rs.4,000 in the presenter. Several seconds later, when the ATM times out and sends an error message to the financial institution, 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
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.

ATM Burglary Attacks
Physical attacks are sometimes attempted on the safe inside the ATM, through mechanical or physical means. The goal is to penetrate the ATM to open the safe door or to make an opening in the safe sufficiently large 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 pickup 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.

Locks and Closing Device
Mechanical locks, Electronic locks, Alarms and Sensors, Ink Dye etc should be used as locks and closing devices in ATMs so as to protect the ATMs from unwanted elements.

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 a monitoring of the ATM and surrounding area can be directed from remote locations at any time.

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Awareness and Consumer Education

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. Financial institutions should confirm that their branch personnel, ATM services providers, and cash handlers, as well, 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. Customers have to carefully review their monthly account statements or to use internet banking to monitor for any uncommon activity on their accounts.

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.

Conclusions

People should be very careful when using an ATM, especially when getting cash. They have to follow these precautionary measures: Always watch for suspicious persons or activity around an ATM.; If you notice anything strange, leave and return some other time.; Even if you have already started a transaction, cancel it and leave that place and after dark take a companion along; Park the vehicle close to the ATM in a well lighted area. Lock the car or the vehicle. If the lights around the ATM aren't working, don't use it; Use the body as a shield while enter the access code so that no one can see us type it. Take all of the transaction receipts. Don't throw them away near the ATM; If you get cash – put it away right away; Don't stand at the ATM and count it; Never accept offers of assistance with the ATM from strangers; Ask the bank for help; If you use a drive-up ATM, your vehicle's other doors should be locked with windows rolled up; Memorize the access code. Don't write it down and / or carry it; Don't use an access code that the same as other words or numbers in the wallet. Never tell the access code to ANYONE. (Including bank employees, the police etc.,) Never lend the ATM card to anyone; Treat it like cash or a credit card; If the ATM card is lost means , notify immediately to the concerned bank or credit union immediately. Accordingly, the use or implementation of some l 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. A good company should allow our customers to provide solutions and recommended approaches to contain such issues as ATM fraud. A 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. Customers should feel secure during their usage of ATMs .

REFERENCE 1 Diebold ATM Fraud and Security White Paper (2002), Diebold, Incorporated, September 2002 | 2 Haruna Issahaku(2013), Customers' Experiences With ATM: A Comparative Analysis Of Gcb And Barclays Bank ATM services, Science Education Development Institute, Volume 3 (3) Mar.: 724 - 734, 2013. | | 3 Anurag Anand Duvey1, Dinesh Goyal2, Dr. Naveen Hemrajani3 (2013), A Reliable ATM Protocol and Comparative Analysis on Various Parameters with Other ATM Protocols International Journal of Communication and Computer Technologies, Volume 01 – No.56 Issue: 06 Aug 2013. | | 4 ATM Machines (2008), The benefits of owning an ATM, An ATM Buyer's Guide, Copyright 2008 ATM Network. | | 5 Richa Tuli Abhijeet Khatri** Anita Yadav*(2012), Comparative Study of Customer | attitude towards ATM of SBI and ICICI bank, IJMT, Volume 2, Issue 8 , August 2012. | 6. www.sbi.co.in |