

ATM Vulnerabilities, Frauds and Crimes



Identifying vulnerabilities in the ATM system is an indispensable skill for the auditors of today. The sheer number of the ATM crimes and their wide variety make it very difficult for any person to grasp the essence of the subject. The author, after analysing thirteen hundred cases, has classified the vulnerabilities into four groups viz., Customer and the Bank being cheated, Machine failure, Security failure and Accidents. This article illustratively covers the point of 'the Customers and the Bank being cheated'. Further, this article is an attempt to equip the auditors that would help them in detecting the loopholes that lay hidden in the ATM system.

The ATM system has totally revolutionalised the banking services by reducing the hassles a customer had to endure in transacting with the banks. But the occurrence of an unprecedented number of ATM crimes has given it quite an amount of notoriety. It has placed a huge burden on the banks in the shape of extra security management. It has also cast on the auditor the additional responsibility of identifying and reporting on inadequate security in the ATM systems.

It will be difficult for an auditor to understand the vulnerabilities of the ATM system without obtaining a good insight into the weaknesses of the ATM system and the wide variety of vulnerabilities arising there from. Once understood, it will give him an ability to identify risks and strengthen his audit procedures.

The present article is an attempt to equip the auditor with precisely this type of information that would help him in detecting the loopholes that lie hidden deep in the ATM system. The analysis given below is based on the results of a detailed study of about thirteen hundred cases reported in news papers and articles from all over the world and in the internet. Most of the aspects of ATM frauds have been included, even though some of them may not be directly relevant from an audit point of view. Some of the cases might look imagined or exaggerated



CA. T.S. Subramanian

(The author is a Member of the Institute. He can be reached at tssm75@yahoo.com)

versions, but each method described here is based on actual facts.

The vulnerabilities in the ATM System

If a person attempts to study the vulnerabilities of the ATM, he would find himself drowned in cases of frauds so large in number and so wide in spectrum that he would not make any head or tail out of it. In order to obtain a proper grasp on the subject, classification under the following groups will help, viz., the risk of losses arising on account of:-

- A. *The bank or the customer being cheated*
- B. *The faults in the machines, software and procedures*
- C. *Inadequacy or failure of security arrangements*
- D. *Unforeseen circumstances and accidents*

In this article the author has discussed the point number A i.e. ***the bank or the customer being cheated.***

A. The Bank or the Customer Being Cheated

This heading falls into further five categories, viz., losses or damages caused by,

1. Outsiders (strangers),
2. Insiders (employees),
3. Technicians (engineers, service providers) and,
4. Bank customers.

1. Outsiders (Strangers)

The card and the PIN are essential for breaking into an account. It is surprising how human ingenuity has been used to find diverse methods for achieving this end.

a) *Shoulder surfing*

'Shoulder Surfing' is the oldest method of collecting the PIN. The crook stands behind the customer, looks over his shoulder, watches his key strokes, and memorises the PIN.

b) *Skimming*

When a person collects the PIN as well as the card details without the knowledge of the customer it is known as 'Skimming'. The customer notices nothing abnormal in the ATM, but, as his card goes through the card slot the crook receives the details of his card. This is achieved by pushing a 'Skimmer' (an electronic device in the shape of oblong black disk which is held in place by spring levers) into the ATM slot. The card has to pass through the skimmer's slot before reaching the ATM card reader. The skimmer reads the data

on the magnetic stripe on the card and transmits them to a device in a parked car. Some skimmers are affixed with tapes just below the card slot. In another model, the body of the skimmer appears just like the original card insertion unit and thrust into the card slot.

Imagine, skimmers have also been found inside the ATMs! Retailers of small sized ATMs turn into crooks and they fix skimmers inside a few ATMs and place them in Malls and Plazas. They are genuine ATMs but they record and store card details and PIN. These are recovered later and used to withdraw funds. In a very recent case police arrested Pascari of Limerick city in Ireland who crafted his own custom-made skimmer equipped ATM machines by ordering the spare parts directly from ATM companies.

An electronically sensitive, thin, plastic sheet pasted within the card slot can also obtain the card details and transmit them.

A notice "*Due to recent fraud attempts at this ATM machine, we require you to swipe your card in the card reader below before inserting your card. We apologise for the inconvenience*" can be found pasted on the ATM. This card reader is a skimmer fixed by the criminal.

The entrance door of an ATM enclosure has a 'card swipe' device for unlocking the door. Crooks replace it with similar looking device with skimmers and collect the card details.

In places where several ATMs are set up in a row, the suspect places "*Do Not Use. Out of Order*" boards before all the ATMs (except the one with the skimmer). The customers are automatically forced to use the ATM with the skimmer.

Miniature pinhole cameras can videograph the finger movements on the keypad and transmit them wirelessly. These are of the size of rupee coin and blend with the colour of the ATM. They are fixed just above the keypad. Sometimes, they are painted to appear like a logo and fixed on the broad frame of the ATM screen itself. Slightly bigger cameras that focus on the keypad are hidden in document folders where a sticker hides the camera from view.

For the customer, the keypad looks normal. But it has been overlaid with a mould in the shape of the original key pad, made out of thick pliable plastic material of the same colour and containing some special electronic circuits. When a person presses a key in the mould, the ATM key also gets pressed. The mould records

the position and transmits the key stroke details to another device. It is called '*Duplicate PIN Pad Overlay*'.

The customer thinks it is a protective plastic covering. But it is a thin transparent, touch sensitive, plastic sheet stuck above the PIN pad. It detects every keystroke and transmits them electronically to another device. This is an advanced version of the PIN Pad Overlay.

c) *False ATM fronts*

Gangs involved in large scale ATM fraud operations prepare duplicate front panels of the ATM and get them fixed over the card insertion and print out units thus covering them up. No one can make out that it is not a part of ATM. The ATM works normally. But the customer's card has to pass through this panel and the skimmer installed within the front panel transmits the card details to a receiver.

d) *Fake ATMs*

It is a common practice the world over to allow private non banking parties to install ATMs in Malls and Plazas. They can be misused to collect card details and the PIN. Parties install ATMs in such public places with bank stickers, hotline numbers etc., pasted all over but without any real connection to any network. Initially cash is disbursed to one and all. Later on, it starts displaying a note of technical error or "No funds". After a few days, they remove the machine, recover the details of cards and PINs and also more than what they had given from the installed skimmer!

e) *Stealing the card*

Snatching from the hand or the bag containing the ATM card and breaking open letter boxes and stealing bank's letters carrying the card or PIN, are the common methods used.

A decent looking gentleman helps an elderly person or an uneducated lady by withdrawing the cash from ATM and gives back the card. But he gives back a fake card. According to a recent report in Odisha, the arrested Balaram Sahoo amassed ₹ 1 crore in two years with this method.

Workers intercept the mails of their employers and steal the cards. Jail Wardens, hospital employees, helpers in old age homes steal ATM cards of their wards.

If a person, in a hurry, forgets to remove the card, the workers around notice it and make use of the active account for withdrawing cash. Some even change the PIN.

f) *Social Engineering*

When a person poses as very responsible and makes another person believe that he could be trusted, it is a case of '*Social Engineering*'. He convinces the card owner that he is safe enough to be trusted with his ATM card and PIN code. He might impersonate as a bank officer, bank employee or a member of the police. Here are some examples to illustrate.

Posing as a Bank Officer

- a. He telephones the customer and says that the bank has cancelled his defective card because of security reasons. He asks for the card but at the same time volunteers to get it collected. He says the old invalid PIN has also to be cancelled before issuing a new one and obtains the PIN. An accomplice collects the card.
- b. He represents himself as an employee of the bank, canvassing for a contest for ATM card holders with huge sums as prize money. He gives them the form, which looks genuine. One of the conditions is that no box should be left empty, and it contains a box for the PIN. He then wants to verify the ATM card is genuine. He swipes them in his portable skimmer.
- c. Posing as a bank security officer, he rings up a client and asks for his cooperation in nabbing a dishonest employee who is trying to steal funds from his account. To execute the trap he asks him to leave his card secretly under the door of the bank after closure of the bank. Next day, he informs him that the employee has been caught red handed and thanks him and tells him that his card is required as evidence and a fresh card would be issued to him. He then collects the PIN by saying that it is needed for cancellation of the old card.
- d. A lady's card gets stuck in an ATM by some installed device. She rings up the emergency phone number given in a

bogus sticker pasted on the ATM. The man on the other side who is an accomplice, identifies himself as the bank employee and offers to issue a new one in its place. For that he needs her PIN and the lady gives it. The card is retrieved later by the crooks.

Posing as Police Officer

- a) First he steals wallets by breaking into lockers in Social Clubs, Sports Club etc. He then rings up the card holder, identifies himself as a police officer, informs him that his card and the wallet had been found with an arrested culprit. He says it will not be returned to him, but to the bank. He says that a small formality needs to be complied with, viz., the PIN has to be recorded in the files. He gives the phone number of the Police Station (his friend's) where he should lodge his PIN.
- b) Dressed as a senior police officer in uniform, with badges, gun etc, driving a big car with flash lights on, accosts elderly persons driving their car and, with his intimidating language checks their belongings, confiscates the ATM card and also obtains the PIN.

Miscellaneous

The criminal, impersonating a senior officer of the super market, phones up a sales girl in the market and informs her that he wants to give her a huge cash incentive for her good work, but confidentially. He wants her ATM card and PIN so that it could be deposited into her account without the knowledge of other employees. The girl gives them.

g) Lebonese loops

This was the first method used when the practice of ATM card capturing started. The culprit positions a thin rigid plastic strip having long wires in the sides (Lebonese Loop), deep inside the ATM slot. When a card is inserted, the 'Loop' prevents its movement and the machine stops. The culprit standing behind him asks him to try entering the PIN twice or thrice, but nothing happens. He memorises the PIN. After the card holder leaves, the culprit pulls out the strip with the help of the wires and the card comes out.

A notice, "*If for any reason your card is retained please enter your PIN number three times and then press cancel button.*" is pasted on the ATM. The customer inserts the card and it is stuck. He enters the PIN three times but nothing happens. He leaves. The crook standing behind memorises the PIN and retrieves the card. The secret is the opaque sheet of plastic placed inside to prevent the card reader unit reading the magnetic stripe.

h) Post & Courier

In Chennai, a customer received an SMS alert of ATM withdrawals, even before he received the card! On investigation, it was found that four persons belonging to a courier company used to hand over the mails to a gang of criminals for a day, who fished out the card details and PIN and returned the mail intact. In US, a Californian postal carrier and a South Brunswick letter carrier were arrested on charges of theft of ATM cards. The interception of the bank letters by the employees in Post Offices and Couriers is a cause for serious concern.

i) Hacking the ATM

In certain banks, dedicated lines are used to connect the ATMs to the host computer along with a separate dial-up line to the host for the use of maintenance engineers. Stealing the confidential number for the dial up line the hacker intrudes into the ATM circuit and converts his friend's card into a Security Card which enables him to do any fraud.

According to the book "ATM Exposed" published by Sailclose Publications 2003, a computer programmer in Taiwan stole 4 million dollars by making more than 7,000 cards by intercepting the communication line to the ATMs.

j) Jackpotting

At the Black Hat Security Conference 2010 in Las Vegas, researcher Barnaby Jack demonstrated, on the stage, high-tech hacks against two genuine ATMs. In one, Jack reprogrammed the ATM remotely over a network; in another attack, he opened ATM's front panel and plugged in a USB stick loaded with his own software. The large audience was shocked to see dozens of crisp bills flow out from both the ATMs.

2. Insiders (Bank Employees)

ATM cash containers are protected by a set of confidential combinations. Only the few trusted members of the staff of the bank or the service providers know them. When the ATM cash disappears mysteriously without any trace, it is rational to conclude that the combinations had been used with or without the connivance of the employees. It might have been leaked out on account of negligence or coercion. It is also possible that they were stolen.

It is a cause for concern that, for the employees in the section dealing with ATM cards and PINs, opportunities exist for collecting PINs and card details. In many fraud cases, the bank employees were found to be the collaborators.

Model Anupama Verma of Mumbai never uses her ATM card and had not even opened the PIN letter. Yet ₹17.36 lakh was withdrawn from her account by using the ATM card 170 times. Two employees of her bank were the culprits. Ralph Elmer of Battle Creek, Michigan never even knew that an ATM card was issued on his account but withdrawals of over \$ 40,000 had been made over several years.

There is a loophole in the despatch section of the bank which sends the card and the PIN to customers. The employees were found to have changed the addresses on the envelope and diverted them to the address of a criminal.

The deposit envelopes in the ATM deposit box were found to have been tampered with and cash removed by collectors. They were also responsible for stealing the amounts swallowed by ATM on account of non withdrawal.

In a bank in Bahrain, an employee who handled the entire ATM operations single handed, swindled money and tried to cover up the fraud by juggling with the daily cash top-ups for the machine.

3. Technicians (Engineers, Service providers)

ATM technicians and service providers like cash fillers etc., are given separate passwords for conducting the ATM operations. These passwords are supposed to be activated only for the brief period of operation. There are instances where, due to negligence, the passwords were not deactivated, and it resulted in the disappearance of cash from ATM.

In one case, an ATM repairman in New York who knew the keystrokes to change the denomination of the issue trays changed \$20 tray into a \$ 5 tray and made the bank issue \$20 instead of \$5.

4. Bank Customers

It is difficult to believe that customers are also indulging in fraudulent activities when they notice any weakness in the system. During the 9/11 disaster when the banks, for humane reasons, decided to open ATMs without their normal controls, the customers stole \$ 15 million within a few days!

In the 'Transaction Reversal' method, the customer removes some notes in the middle of the stack when the machine delivers a stack of notes, and waits. The machine swallows the rest of the notes as unclaimed, but there would be no record of the shortage anywhere.

In a recent ₹1 crore fraud involving Federal Bank and other banks this method was used. The gang members used to demand a withdrawal of ₹10,000 from ATM of Federal Bank. But they used to take only ₹ 9,900 and leave the last ₹100 note inside the ATM. The ATM machine would retrieve the note, and would flash a message of 'failed transaction' in the software system of the private bank whose ATM card was used for withdrawal. Their accounts never got debited.

In ATMs where cheques are accepted as deposits, a huge number of frauds have been executed by depositing cheques on accounts without balance and withdrawing cash against them.

Modifying the ATM

Chinese criminals used an unusual method. They cut the cash conveyor belt inside the ATM so that the undelivered cash falls within the machine. After the departure of the client, they removed the cash.

Miscellaneous

In certain ATMs, the customer has to swipe the card and then remove it. At the end, he has to hit a key to exit. If the key is not pressed, the machine waits for 60 seconds before closing. The Daily Telegraph Kolkata reported that one Alok knew this secret and used to transact as soon as the customer left. Though he failed on most occasions, but few times he succeeded to fetch a whopping sum of about ₹4 lakh.

Phishing

Phishing technique is mostly used by hackers to obtain confidential details of bank password via email. But sometimes they collect ATM PINs too. The customer believes in a bogus email looking exactly like his banker's asking for personal details, password PIN etc., He blindly complies with the request. ■