ATM FRAUD AND COUNTER MEASURES

PRESENTED BY J. PATRICK OKIRING
GENESIS OF ATMs

An automated teller machine was first introduced in 1960 by City Bank of New York on a trial basis. The concept of this machine was for customers to pay utility bills and get a receipt without a teller. After being proven to be useful, it was adopted largely by financial institutions.
BENEFITS OF ATM
BENEFITS OF ATM

TO CUSTOMERS

- Enables convenient access to round the clock financial services for persons who wish to check their account balances, withdraw and deposit money into and from their accounts, and bill payments.
- Less burden of having to carry around loads of cash for account holders. This is especially useful for travellers.
- Better personal security
BENEFITS OF ATM

TO FINANCIAL INSTITUTIONS

- Provides a revenue stream line for financial institutions in card and transaction fees.
- Reduces customer queues in the banking halls and pressure on staff.
- Reduces human errors in transactions, ex. the correct amounts being dispensed.
TYPES OF ATM CARDS
TYPES OF ATM CARDS

Basic

- This is a regular card that is used at any ATM machine to withdraw and deposit money, check account balance and funds transfers.
- Some ATM cards in this category have a few more uses relating to loan payments and cash advances.
TYPES OF ATM CARDS

Debit Card

- An ATM debit card has all the features of a regular ATM card with the added features of enabling purchases at any store or online. Each time a transaction is done, money is taken from the account the card is linked to.
Credit Cards

- This type of card has all the debit card features and is attached to a checking account and a line of credit. This allows for the customer’s account with insufficient funds, to draw from their credit line to be paid back with interest when funds are made available.
ATM CARD
FRAUD
A Global Problem

ATM Fraud is happening on a global scale. As the world comes closer together, a bank customer in Uganda will have a run-in with a criminal from Bulgaria. And a scheme that works in the UK today may end up in Uganda sooner, rather than later.
Testimony
TYPES OF ATM CARD FRAUD
**TYPES OF ATM CARD FRAUD**

**Card trapping**

- Involves placing a device directly over or into an ATM's card reader slot. These devices are designed to retain cards after customers insert them.
This fraud involves placement of money traps or false presenters in front of an ATM dispenser.

During the course of an otherwise normal transaction, an ATM dispenses notes into the trap rather than present the money to the customer.

Assuming the ATM has malfunctioned, the customer leaves. The criminal returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer.

Cash trapping commonly succeeds with insider involvement.
Here, the victim is tricked into revealing his/her authentication information (PIN). It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their ‘Bankers’. The user ends up divulging his card sensitive data to the rogue site.
Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM. Magnetic stripe cards are very vulnerable to this type of attack.
Operational Fraud

- **Dispenser manipulation**
  In this case, the ATM is set up to dispense big denominations as smaller ones, thereby giving out more money than should be dispensed. This is possible by insider help or remote commandeering.

- **Fraudulent issuance**
  Here, a bank employee deliberately issues the card(s) and PIN(s) to wrong claimants in disregard of the issuance verification procedures.
Operational Fraud continued ……

- Fraudulent placements

This is a case where ATM card production requests are made without any indication of interest from the account owner. This is commonly done by bank employees.
Physical Attack

ATM physical attacks are attempted with the aim at the safe inside the ATM, through mechanical or thermal means with the intention of breaking the safe to collect the cash inside. Some of the most common methods include:

- Ram raids
- Explosive attacks and cutting
- Robbery when ATMs are being replenished or serviced.
Shoulder Surfing

- Shoulder surfing involves observation as a person taps onto an ATM PIN pad. Criminals typically position themselves close to legitimate ATM customers to watch covertly as the customer enters his or her PIN.

- Shoulder surfing is also possible through the installation and use of miniature video cameras aimed to record PIN entry.
Skimming

This is the most popular/common ATM fraud. In this type of ATM fraud, the perpetrator(s), steal the card owner’s authentication data using a device labeled skimmer. The stolen data is then used to make counterfeit cards that are used to draw money from the victim’s account.
Where to spot a card **skimming** device

Region 1. Light diffuser area

Region 2. Card reader entry slot

Region 3. Speaker area

Region 4. ATM side fascia

Region 5. ATM keyboard area
What do skimming devices look like?

Here, we have an example of a skimming device that can be installed within the ATM fascia.
What do skimming devices look like?

Removal of a skimming device from a card reader slot. The device was fitted over the card reader throat.
What do skimming devices look like?

Can you tell if this ATM fascia piece (located above the screen) has a skimming device installed within? You cannot really tell can you!
What do **skimming** devices look like?

A closer look at a removed ATM fascia piece.
What do **skimming** devices look like?

A closure look at the inner part of the fascia piece removed, reveals the PIN capturing device.
What do skimming devices look like?

Another example of a skimming device installed on the inner side of the light diffuser fascia piece (above the ATM screen). Can you see the camera?
What do **skimming** devices look like?

A closer look at the inner part, reveals that a mobile phone camera was used as a skimming device, with the information being transmitted via a wireless device.
What do **skimming** devices look like?

A brochure holder is placed on the side of the ATM fascia wall. Can you spot a PIN capturing device?

…
What do skimming device look like?

Upon closer inspection of the merchandising unit, you can clearly see the pin hole camera installed on the bottom side, capturing an image of the keypad.
What do *skimming* devices look like?

The last area of focus is the ATM keyboard fascia.
Offenders are known to place the skimmer plate on top of the existing keyboard or near it.
COUNTER MEASURES
Track ATM fraud else where

The Banking Industry must consider a global view of ATM fraud by tracking crimes related to ATMs in every part of the world and proactively develop solutions to minimize their materialization and the related losses.
II. Leverage on technological improvements

- Deployment of biometric capabilities in ATMs authentication systems. With biometrics, fraudulent incidents can be minimized, as an added layer of authentication is introduced that ensures that even with the correct pin information and possession of another person's ATM card, the user's biometric features cannot easily be faked.
- Migrate to EMV-chip based card readers as magnetic strip is vulnerable to skimming
- Activate E-alerts so as to notify the account owner of movement on his/her account, especially debits.
- Consider where viable, ink stain technologies that will ruin and make unusable any removed banknotes.
III. Address human resource issues

- Train the staff handling card requests and PIN issuances.
- Establish clear job descriptions and accountabilities for the staff handling card/PIN requests and issuances.
- Review remuneration of front office staff.
IV. Rethink what constitutes Physical security

- Engage the firms providing physical security to interest them into broadening their understanding of security requirements that are adaptive to human behavior.
- Use of effective surveillance systems; CCTVs, sensors that detect physical attacks, especially in remote locations.

V. Stock management

- Institute effective oversight over card operations-origination, production, storage and issuance.
- Consider stock management and tracking systems
VI. Get to know the appearance of your ATM room.

VII. Familiarize yourself with the look and feel of your ATM fascia. Particularly pay attention to all of the touch and action points. (e.g. keypad, card entry slot, lighting diffusers)

VII. Inspect the front of the ATM for unusual or non standard appearance. Scratches, marks, adhesive or tape residues could be indicators of tampering.

VIII. Report any unusual appearance immediately to nearest Branch.
IX. .................................................. your contribution
By being vigilant you can play a part in reducing the risk of a skim attack!

SECURITY IS EVERY ONE’S RESPONSIBILITY
EYALAMA!!!