Crime Prevention Section

ATM SKIMMING & RADIO FREQUENCY IDENTIFICATION

COMMUNITY AFFAIRS BUREAU

Raymond W. Kelly
Police Commissioner

D.I. James Klein, C.O. Crime Prevention Section

ATM (Debit Card) Skimming

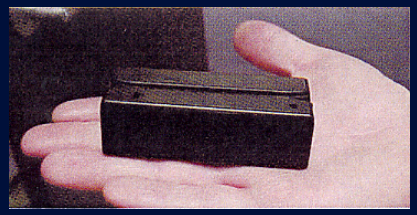
In order to clone and access debit card accounts, suspects must obtain both the track information of the debit card and the PIN (Personal Identification Number) associated with the debit card account.

Normally, (2) electronic devices are needed in order to obtain both pieces of information:

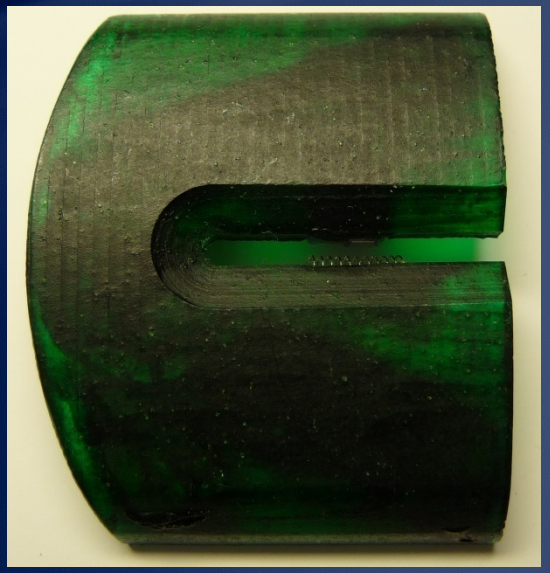
- **ATM Skimming Device**
- **PIN Capturing Device**

Skimming Devices

Electronic "skimming" devices are used to capture un-suspecting customers' track information (back of credit and debit cards) while the card is being used for a legitimate transaction.



Sample ATM Skimmers



Before and after….

Can you tell the difference? A skimming card reader placed on an ATM.

Caution! This is the skimming card reader.

ATM Lobby Door Skimmers

Instead of placing the Skimming Device directly on the ATM machine, skimming devices can be placed at the ATM Lobby Door Access Device.

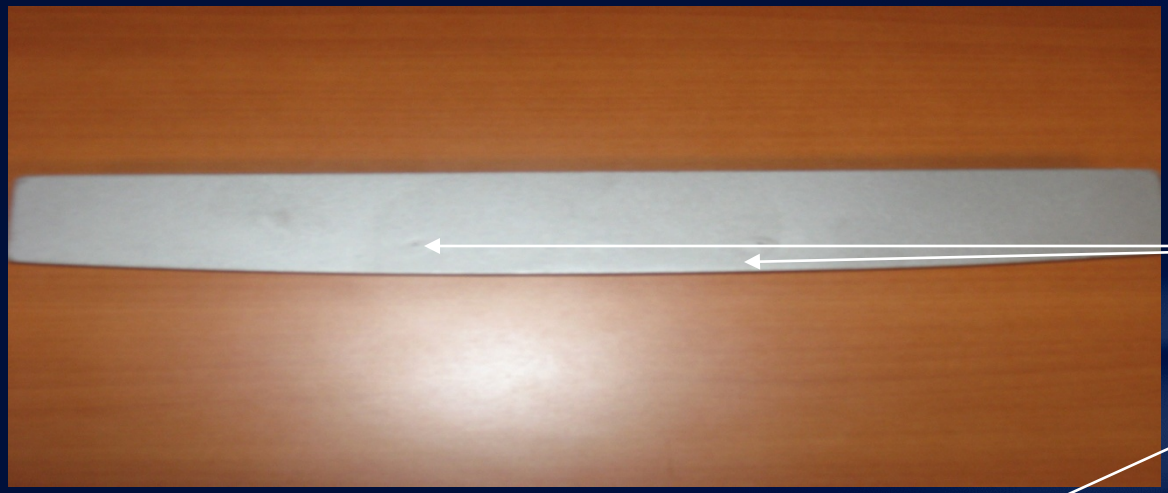
Customers using their debit card will swipe their cards through the installed device and the track information will be captured.

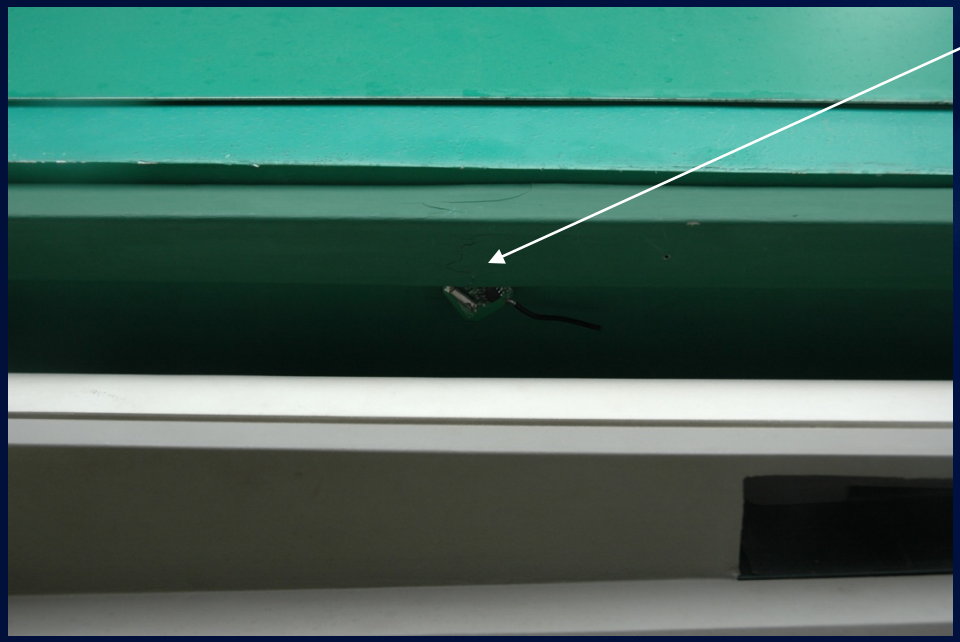
ATM Lobby Door Skimmer location

PIN-Capturing Devices

- Types
  - Pinhole cameras
  - Cellular telephone components
  - Skimmer plates
  - Bluetooth
- Where installed
- How they work

Sample Pin-Hole Cameras/Camera Strips



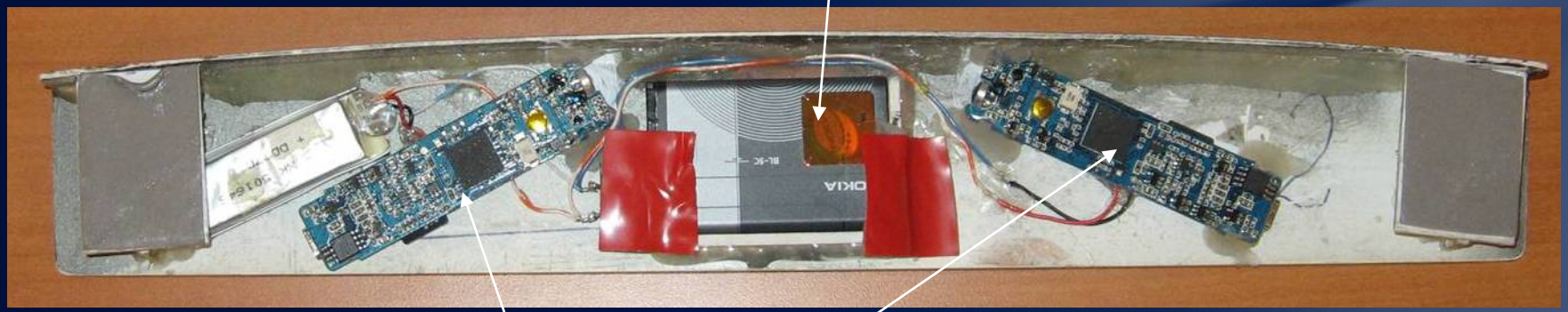



WARNING
This ATM is security monitored and fitted
with an Anti Removal Device
Sorry, this machine
is temporarily
out of service


WARNING
This ATM is security monitored and fitted
with an Anti Removal Device
Sorry, this machi

Components of Norwalk Device

Nokia Cell Phone
Battery



Camera devices

General Overview

PIN Capturing Devices (con't):

- **ATM Keyboard Skimmer Plates can also be used to capture customers PIN #'s.**
- **The plates are placed over the factory installed PIN number plates of the ATM.**
- **The plates record the customer's PIN and the device is later removed.**

ATM Skimmer Plates

General Overview

- **Components of cellular phones can be used as camera/recording devices to capture customers PIN #’s:**

Combined Skimmer/Camera

An all-in-one skimmer/camera contains both a skimmer and PIN Capturing Device.

Combined Skimmer/Camera

Blue Tooth Capable Skimming Devices

- Blue Tooth technology now being used with skimming devices.

- Blue tooth components are embedded in the skimming device and allow retrieval of track and PIN information without having to remove the devices.

Blue Tooth Devices


KL

Using the Captured Information

The track information on the skimmer is downloaded onto a computer and then re-encoded on counterfeit/stolen debit/credit cards and/or any other card with a magnetic strip.

Radio-frequency identification (RFID)

- **The wireless non-contact use of radio-frequency electromagnetic fields, to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Some tags require no battery and are powered and read at short ranges via magnetic fields**

Radio-frequency identification (RFID)

- Technology used to eliminate need for cards to be physically handled or swiped.
- Possible drawback, unauthorized persons might use RFID readers of their own to obtain information.
- Cards can be read from as far as a few feet away.

Devices/Examples

Preventative Measures

- Leave Your RFID Credit Cards at Home
- Put Two RFID Credit Cards in Your Wallet
- Put a Piece of Tin Foil in Your Wallet
- Keep An Eye on Your Credit Card Statements

ATM Safety Tips

- Be aware of suspicious people outside and inside of ATM location
- Don’t switch/leave ATM machines without closing transaction fully.
- Block the view of bystanders when doing your transaction. Use mirrors positioned at the ATM to see behind you.
- If you feel someone is looking over your shoulder, cancel transaction and leave immediately.

ATM Safety Tips Cont'd

- Use well lit, well populated ATM's
- Avoid ATM's that have unlocked doors or are directly out on the street.
- Put your money away, take your card and receipt before exiting the ATM.
- Use your card exclusively for your entry only, make sure door closes directly behind you. Do not open door for strangers

CONCLUSIONS

- Be careful with you personal/financial info
- A simple scheme can be a financial disaster
- A large degree of anonymity
- Penalties not very severe
- Excellent means to finance other “ventures” – terrorism?
- When you swipe your credit/debit card make sure you are logged off before completing transaction

CREDIT BUREAUS

- Equifax
  800-525-6285, www.equifax.com
- Experian
  888-397-3742, www.experian.com
- Transunion
  800-680-7289, www.transunion.com
- Federal Trade Commission
  877-ID-THEFT, www.consumer.gov/idtheft

Community Affairs Website

- COMMUNITY AFFAIRS SECTION OF THE NYPD WEBSITE
- Download Crime Prevention materials.
- Sign up for the Community Affairs Bureau E-Alerts.
- Email: communityaffairs@nypd.org
- www.nypdcommunityaffairs.org

- Like the NYPD on Facebook 
- Follow the NYPD on Twitter 
- Watch us on YouTube 


QUESTIONS?!?!

Contact Us :

Crime Prevention Section
34 ½ East 12th Street 3rd Floor
New York, N.Y. 10003
Telephone # 212-614-6741
Email: communityaffairs@nypd.org
www.nypdcommunityaffairs.org

THANK YOU FOR YOUR TIME AND ATTENTION !