SPECIAL ALERT: BEWARE OF ATM SKIMMING

June 24, 2010

What is ATM Skimming?

Across the nation, criminals have developed electronic devices that attach to bank Automatic Teller Machines (ATM) that are designed to capture the debit card information on the card's magnetic strip, and record the victim's personal information number (PIN) as he or she conducts the ATM transaction. Both bank vestibule and drive-up ATMs are targeted for attack by these schemes.

The victim's information captured by the devices is then used to "clone" the victim's card. "Cloned" cards may be new credit card blanks, old credit/debit cards, used gift cards and other types of cards utilizing magnetic stripes. The victim's information is re-encoded on the magnetic stripe on the clone card. The "cloned" cards are then fielded out to "passers" who visit ATM's at other banks or branches to withdraw cash, usually several weeks or months after the compromise has occurred. The scheme is usually the work of organized crime groups and any financial institution may be targeted.

How it Works:

The devices are designed to closely resemble the card reader, keypad and other devices or parts on the ATM, and are not readily detected unless you know what to look for. Two devices are commonly installed on the ATM by the criminal to accomplish the compromise.

1. The first is the "skimmer," a device that records the information on the magnetic stripe on the rear of the card. The skimmer fits neatly over the ATM's card reader. As the victim inserts his or her card into the ATM the skimmer it passes through the skimmer which records the magnetic stripe information.
2. PIN's can be recorded by two different methods.
    a. One way is a keypad "overlay" that looks like a key pad and designed to cover the existing ATM keypad. As the victim punches in his PIN, the overlay allows the PIN to be recorded by both the overlay's circuitry and the ATM, permitting the transaction to be completed normally.
    b. A second manner is the installation of a "pinhole" camera in the proximity of the ATM keypad to record the victim keying in the PIN. The

camera may also be mounted in a fake pamphlet box or fascia piece on the ATM with a view of the keypad.

What to Do:

- Shield the ATM keypad with your hand as you key in your PIN.
- Look for adhesives such as glue or tape. Devices may be attached using glue or double sided tape, and in some circumstances, holes were drilled into ATM fascia's to mount the equipment. The skimmers may be pulled off quite easily.
- Fake PIN pads or overlays
- Any unusual instruments or objects that do not appear normal.
- Loose or missing screws around the ATM fascia or light fixtures.
- **DO NOT** use, touch or handle the device or ATM. Contact the bank manager immediately, or call (631) 852-COPS (2677) if the bank is closed and wait for police to respond.

The photographs below are some examples of "skimming" devices found on ATM machines

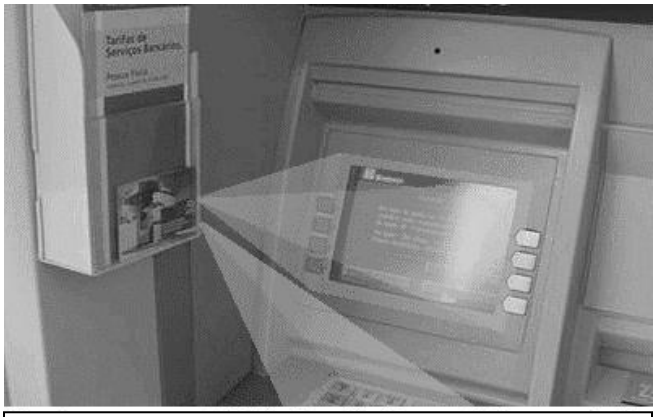
Skimmer over the ATM's card reader.

Fake skimmer and keypad installed

Key Pad Overlay and skimmer

Pinhole Camera in Pamphlet Holder

Pinhole camera in ATM fascia over screen w/ view of keypad



Pinhole camera in holder with view of keypad

The micro camera mounted in the side of the fake pamphlet box can view the KEYPAD and MONITOR, and transmits wireless pictures up to 650 feet away.