NYPD
New York City Police Department

ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer
The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is "skimmed," or stolen, and usually stored on some type of electronic device.

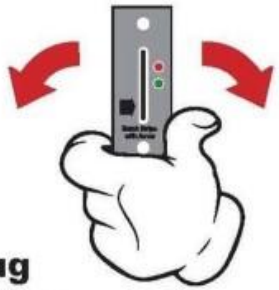
3 Keypad overlay
The use of a keypad overlay—placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.

-Inspect the ATM, gas pump, or credit card reader before using it…be suspicious if you see anything loose, crooked, or damaged, or if you notice scratches or adhesive/tape residue.
-When entering your PIN, block the keypad with your other hand to

ATM Skimming.

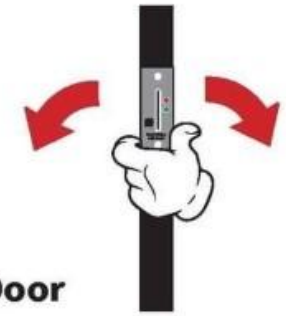
The Scam.

ATM "Skimming" occurs when a criminal attaches a phony card reading device over the real card reader located either at the lobby entrance door or on the ATM machine, the phony device looks identical to the real device and is equipped with electronic recorders that will capture the financial information from your card. This data is later used to create "cloned" cards which will later be used to withdraw money.



Tug

These devices are usually attached with two sided tape and can be discovered by simply tugging on areas where the card must be swiped.



Door

Skimming device can also be affixed to the card reader at the entrance door to the ATM.

What Can I Do?

Before Using

Give the card reader a tug. See if it feels loose or out of place. Inspect the ATM, gas pump, or credit card reader before using it. Be suspicious if you see anything loose crooked or damaged, or if you notice scratches or adhesive tape/residue.

Be Aware

Be careful of ATMs in tourist areas - they are a popular target of skimmers

Money Trap

Be aware of "Money Trapping", where the criminal attaches a device to the cash dispenser "trapping" the customer's money and retrieves it after the customer leaves the ATM area.

Protection

When entering your PIN, cover the keypad with your other hand to prevent possible hidden cameras from recording your number.

Report It.

Immediately report any skimming devices to your financial institution and the NYPD by calling 911.

NYPD

www.nyc.gov/nypd