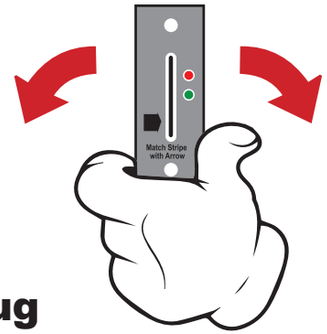
ATM Skimming.

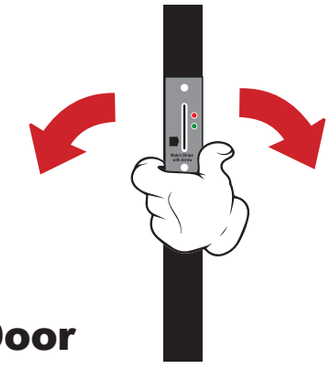
The Scam.

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.

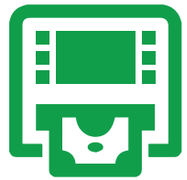
What Can I Do?

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