

# PROTECT AGAINST ATM FRAUD



1

**Selecting an ATM.** If you are traveling and you have to use an ATM, make sure you choose the right ATM. You will want to choose an ATM in a well-lit area and where it would get a lot of foot traffic. If you have the option, choose an ATM that is located inside a bank building versus one on the street. Avoid using stand alone ATMs that look like they are owned privately. These are more susceptible to Fraud.

2

**Card-Reader Overlays.** The most common ATM skimmer is the card-reader overlay. It is made of plastic and fits over the slot where you insert your card. As you insert your card, the device reads the data from your card and stores it. Before inserting your card, look at the card reader for signs it has been altered. Be suspicious if your card doesn't easily go into the machine or if the card reader appears loose, crooked or damaged, or if you notice scratches, glue, adhesive tape or other possible signs of tampering.

3

**Pin Capture Overlays.** Criminals have been known to attach dummy keypads over an ATM's real keypad to record and capture PIN numbers as they are entered. The keypad might be fake if it looks too thick or different from what you're used to seeing.

4

**Fake ATM Faceplates.** Some thieves go as far as placing a fake ATM cover that could contain card-reader overlays, hidden cameras and PIN-capture overlays over some or all of a real, fully operating machine. The best way to determine if an ATM has a false cover is to look for flaws like loose wires, seams that are not flush and slots or keypads that look out of place.

5

**Pay attention to your accounts.** Keep a close eye on your account for any unfamiliar transactions -- regardless of how small they might be -- and immediately follow up with your bank if something seems amiss.