FRAUD AND SKIMMERS PREVENTION

First Financial
FEDERAL CREDIT UNION

Taking a trip to the ATM?
Beware of Skimmers

In the fall of 2015, two brothers from Bulgaria were charged in U.S. federal court in New York with using stolen bank account information to defraud two banks of more than $1 million.

Their scheme involved installing surreptitious surveillance equipment on New York City ATMs that allowed them to record customers' account information and PINs, create their own bank cards, and steal from customer accounts.

Skimming typically involves the use of hidden cameras (top) to record customers' PINs and phony keypads (right) placed over real keypads to record keystrokes.

What these two did is called "ATM skimming"—placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine. ATM skimming is a growing criminal activity that some experts believe costs U.S. banks hundreds of millions of dollars annually.

How Skimming Works

The devices planted on ATMs are usually undetectable by users—the makers of this equipment have become very adept at creating them, often from plastic or plaster, so that they blend right into the ATM's facade. The specific device used is often a realistic looking card reader placed over the factory-installed card reader. Customers insert their ATM card into the phony reader, and their account info is swiped and stored on a small attached laptop or cell phone or sent wirelessly to the criminals waiting nearby.

In addition, skimming typically involves the use of a hidden camera, installed on or near an ATM, to record customers' entry of their PINs into the ATM's keypad. There have also been instances of, instead of a hidden camera, criminals attach a phony keypad on top of the real keypad...which records every keystroke as customers punch in their PINs.

Skimming devices are installed for short periods of time—usually just a few hours—so they're often attached to an ATM by nothing more than double sided tape. They are then removed by the criminals, who download the stolen account information and encode it onto blank cards. The cards are used to make withdrawals from victims' accounts at other ATMs.

How to Avoid being Skimmed

- 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 prevent possible hidden cameras from recording your number.
- If possible, use an ATM at an inside location (less access for criminals to install skimmers).
- Be careful of ATMs in tourist areas as they are a popular target of skimmers.
- If your card isn't returned after the transaction or after hitting "cancel," immediately contact the financial institution that issued the card.

What To Look For

1 Hidden camera

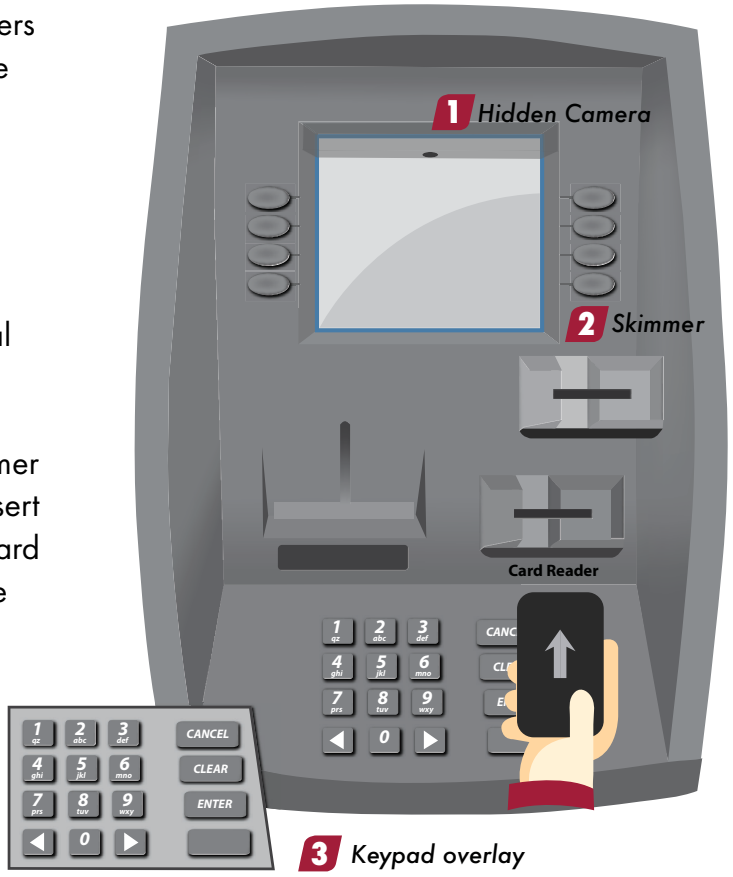
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light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

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fi ts 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.

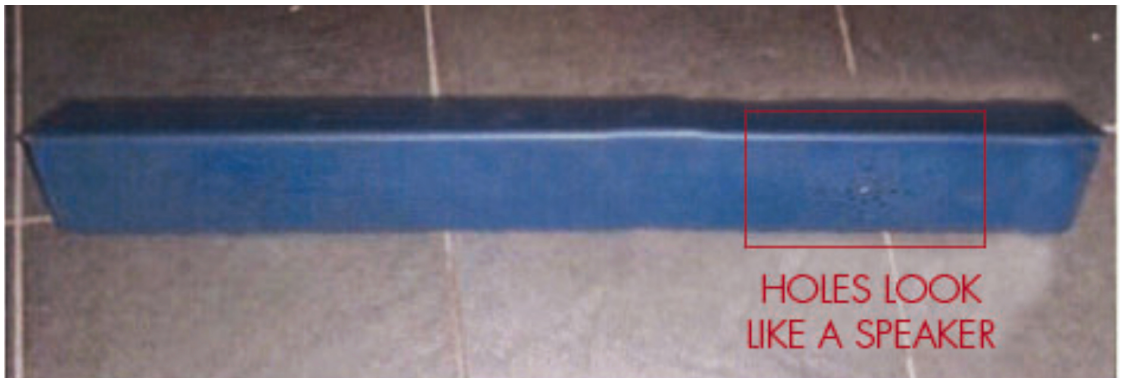


What appears to be a normal speaker above the keypad is actually a hidden camera to read your pin number

Looks like a normal brochure holder — notice how thick the holder is — this is to allow the video camera to hide inside

Removal of the fake device from the ATM machine

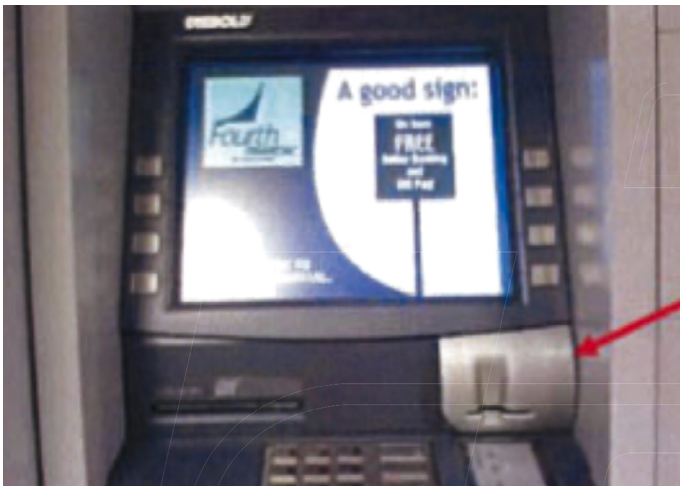
On the interior side of the holder, a hole is cut out to allow the video camera to view your pin number and account number



A smaller device to read your pin number

Inside is the video camera which captures your information

Look for changes in ATMs you frequent. This particular card reader has a green light to guide you. When the fake card reader is added, it covers the light.



First Financial
FEDERAL CREDIT UNION

732.312.1500

firstffcu.com