Skimming

Skimming occurs when devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts. It is estimated that skimming costs financial institutions and consumers more than $1 billion each year.

Fuel Pump Skimming

- Fuel pump skimmers are usually attached in the internal wiring of the machine and aren't visible to the customer.
- The skimming devices store data to be downloaded or wirelessly transferred later.

Tips When Using a Fuel Pump

- Choose a fuel pump that is closer to the store and in direct view of the attendant. These pumps are less likely to be targets for skimmers.
- Run your debit card as a credit card. If that's not an option, cover the keypad when you enter your PIN.
- Consider paying inside with the attendant, not outside at the pump.

Report

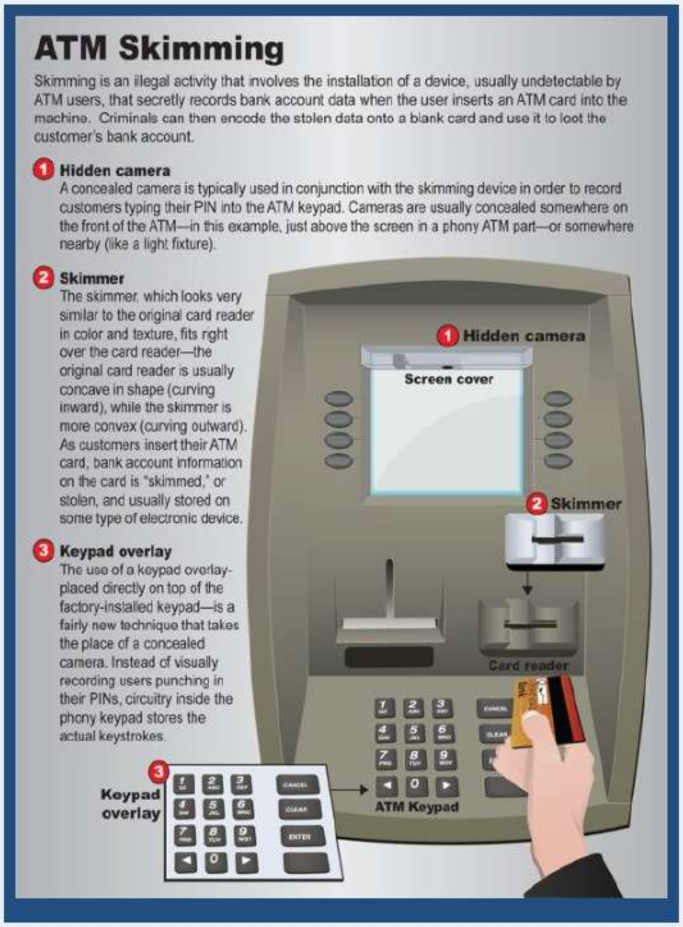
If you think you've been a victim of skimming, contact your financial institution immediately.

ATM and POS Terminal Skimming

- ATM skimmer devices usually fit over the original card reader.
- Some ATM skimmers are inserted in the card reader, placed in the terminal, or situated along exposed cables.
- Pinhole cameras installed on ATMs record a customer entering their PIN. Pinhole camera placement varies widely.
- In some cases, keypad overlays are used instead of pinhole cameras to records PINs. Keypad overlays record a customer's keystrokes.
- Skimming devices store data to be downloaded or wirelessly transferred later.

Tips When Using an ATM or POS Terminal

- Inspect ATMs, POS terminals, and other card readers before using. Look for anything loose, crooked, damaged, or scratched. Don't use any card reader if you notice anything unusual.
- Pull at the edges of the keypad before entering your PIN. Then, cover the keypad when you enter your PIN to prevent cameras from recording your entry.
- Use ATMs in a well-lit, indoor location, which are less vulnerable targets.
- Be alert for skimming devices in tourist areas, which are popular targets.
- Use debit and credit cards with chip technology. In the U.S., there are fewer devices that steal chip data versus magnetic strip data.
- Avoid using your debit card when you have linked accounts. Use a credit card instead.
- Contact your financial institution if the ATM doesn't return your card after you end or cancel a transaction.



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.

SOURCE: FBI (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/skimming)