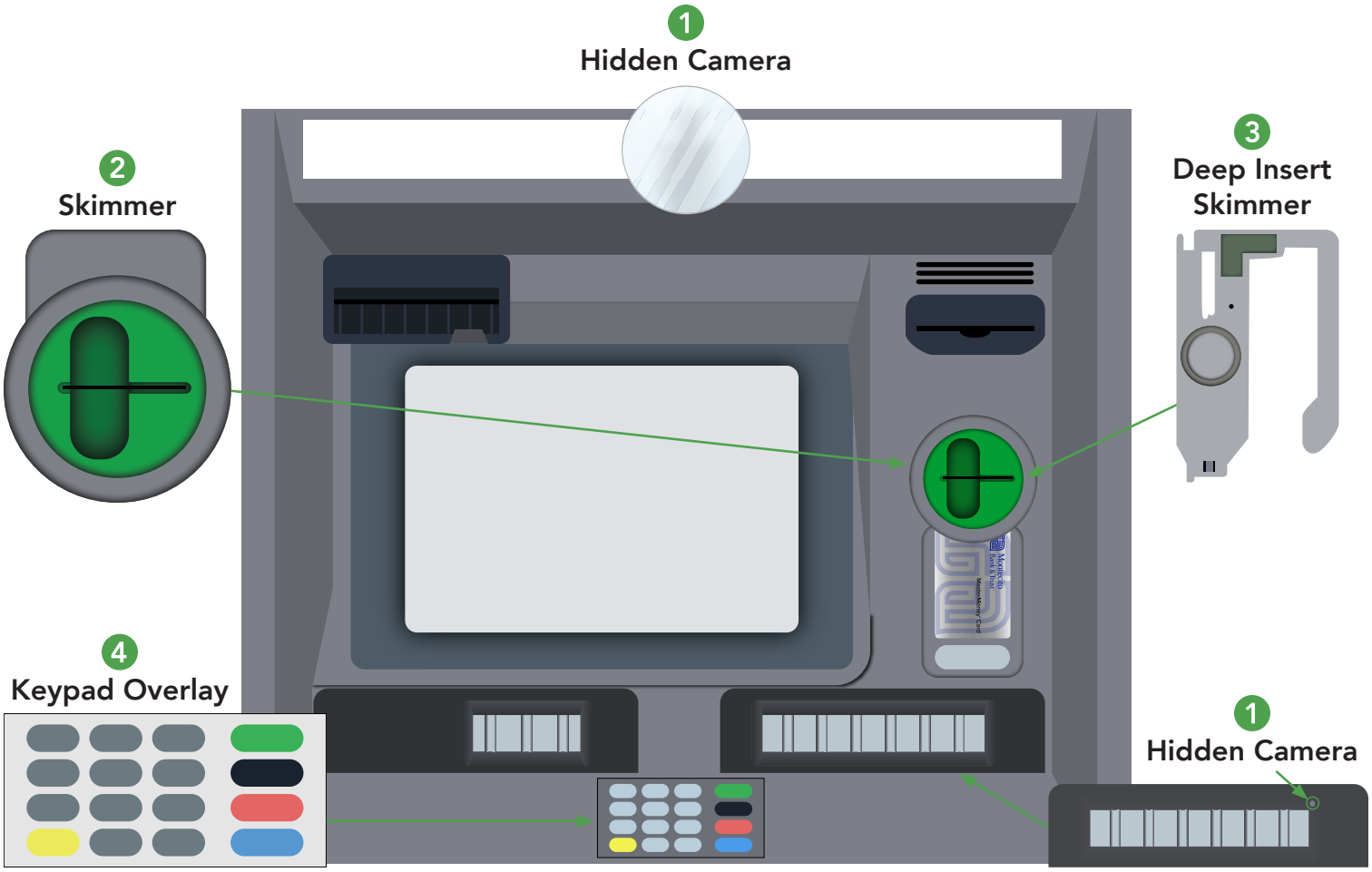
ATM Skimming

Skimming is an illegal activity that involves the installation of a device, sometimes detectable by ATM users, that secretly records bank account data onto a bank card and uses it to gain access to the customer's bank account.



1. Hidden camera

A concealed camera is commonly used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras may be concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or a pin hole on the cash dispenser.

2. Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader. As a customer inserts their debit card, bank account information on the card is "skimmed" or stolen, and usually stored on some type of electronic device.

3. Deep Insert Skimmer

There has been a rapid rise in reports of what are called "deep insert skimmers," wafer-thin fraud devices made to be hidden inside of the card acceptance slot on a machine. These are completely hidden from the customer at the front of the machine.

4. Keypad overlay

The overlay is placed directly on top of the factory-installed keypad. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad can be used to store the actual keystrokes.

What is "skimming?"

Card cloning, or "skimming" as it is sometimes called, is a technique where someone obtains your debit card details, copies them onto a bogus card and begins using the counterfeit card.

What are the most common places card skimming can occur?

1. *The gas pump:* Some thieves will install a small electronic reader (which can be seen if closely observed) on the existing card reader. This additional illicit reader will store your debit card information as you swipe your card to activate the gas pump. They'll then come back later and remove the reader in order to make use of the stolen debit card information.
2. *ATM machines:* This is a popular choice for the same reasons as the gas station. Thieves can place a skimmer on a card reader outdoors and leave it to collect your information.

How can you detect and avoid having your card skimmed at the ATM or gas pump?

1. *Inspect the card reader and the area near the PIN pad:* If you think the device doesn't look like it matches the machine's color and style, it might be a skimmer.
2. *Look at other nearby gas pumps or ATM card readers to see if they match the one you are using:* Does the setup look different? If so, it might be a skimmer.
3. *Trust your instincts:* If in doubt, use another pump or ATM somewhere else. If you are at a local branch and suspect someone has tampered with an ATM, please notify a bank employee of your suspicions.
4. *Avoid using your PIN number at the gas pump:* It's best to choose the credit option that allows you to avoid entering your PIN in sight of a card skimmer camera.
5. *When using an ATM, cover your hand as you type your PIN:* This will help keep a camera from catching a view of what you're typing.
6. *Keep an eye on your accounts:* Report any suspicious activity immediately if you suspect that you might have had your card skimmed.

So you've been skimmed, what are your next steps?

1. Call the police, file a police report. Keep a copy of the report for your records.
2. Contact your bank or debit card issuer immediately and tell them your card data has been stolen. File a claim for any unauthorized transactions.