

*Darienite*

*News for Darien*

*<http://darienite.com>*

---

## How to Lower Your Chance of Getting Scammed by an ATM Skimming Device

**Author :** David Gurliacci

**Categories :** [Public Safety](#)

**Tagged as :** [Crime Prevention](#), [Crime Prevention 2017](#), [Crime Prevention Advice](#), [Crime Prevention Advice 2017](#), [Crime Prevention Tips](#), [Crime Prevention Tips 2017](#), [Larceny from a Bank](#), [Larceny from an ATM Skimmer](#)

**Date :** February 22, 2017

You can make it less likely that you'll become the victim of a skimming device placed on an ATM by a thief by following these steps, according to the FBI.

Here's the FBI's [list of tips](#):

- **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** — 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. [*Editor's note: Having each of your card's phone numbers and card numbers handy in your wallet would make that easier.*]

An additional point: "ATMs aren't the only target of skimmers—we've also seen it at gas pumps and other point-of-sale locations where customers swipe their cards and enter their PIN." [*Editor's note: The Connecticut Department of Consumer Protection has some advice about [protecting your card information when buying gas.](#)*]

# 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.



*Like this article? ...*

- Sign up for the [Darienite.com weekday newsletter](#).
- Like [Darienite.com on Facebook](#).
- Follow [Darienite.com on Twitter](#).

---

From [Darienite.com](#):

### **What Skimmers Are and How They Work**

Skimmers typically are carefully constructed covers that are meant to fool ATM users into thinking that they're inserting their cards into the ATM. (Some skimming devices have been found that slip inside the card slot.)

Instead, when a customer inserts a credit or debit card and provides PIN codes or passwords, the skimmer records the information on the magnetic strip of the card. The skimmer may use a hidden camera to get the PIN code. The skimmer passes on the information to the ATM, or allows the card to pass it on, but then uses the information to remove money from the account connected with the card.

Skimming devices, to be effective, are created with extreme care, and it can be difficult for ATM users to spot them.

***See also:***

- [How to Spot and Avoid Credit Card Skimmers](#) (PC Magazine, April 5, 2016)
- [Four Tips to Protect You from ATM Thieves](#) (Bankrate.com)
- [How to Spot ATM and Pin Skimming Devices](#) (Ossian Bank)
- [All About Skimmers](#) (Krebs on Security blog, 2010 to 2016 — more than you probably want to know, and much of it depressing)