# Skimming

Skimming occurs when devices illegally installed on or inside ATMs, point-of-sale (POS) terminals, or fuel pumps capture card data and record cardholders' PIN entries.

Criminals use the data to create fake payment cards and then make unauthorized purchases or steal from victims' accounts.

It is estimated that skimming costs financial institutions and consumers more than $1 billion each year.

**Report Skimming**

Visit ic3.gov, the FBI's Internet Crime Complaint Center (IC3), to report skimming.

## Skimming Scams

### Fuel Pump Skimming

Fuel pump skimmers are usually attached to 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. You should also examine the keypad before use for any inconsistencies in coloring, material, or shape. These inconsistencies might suggest that a foreign device (keypad overlay) is present.
- Consider paying inside with the attendant, not outside at the pump.
- Tap the card instead of swiping or inserting it when paying at the pump (if the card and terminal allow for it). Tap-to-pay transactions are more secure and less likely to be compromised.

### ATM and POS Terminal Skimming

In these scams, ATM skimmer devices are inserted in the card reader or otherwise installed within the terminal. However, some skimmer devices may fit over the terminal's card reader or be situated along exposed cables at freestanding ATMs (such as those found at convenience stores).

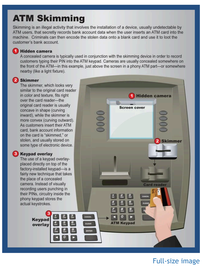
Pinhole cameras installed on or around ATMs record a customer's PIN entry. Pinhole camera placement varies widely.

In some cases, keylogging keypad overlays are used instead of pinhole cameras to records PINs. These overlays record a customer's keystrokes.

POS skimming devices, such as those capturing EBT card data, are generally designed as overlays to the POS terminal and have wireless transmission capabilities. These may be present in any market, convenience store, or retailer.

It only takes seconds to install a skimming device. Fraudsters may seek to distract store clerks—such as by requesting items from behind the counter—to accomplish this.

Skimming devices store data to be downloaded or wirelessly transferred later. Some of these devices transmit the data wirelessly in real time to nearby devices.




Full-size image

### Electronic Benefits Transfer (EBT) Card Skimming

EBT card data has become a key target for many skimming groups and criminals since at least 2021, through card skimming and other tactics.

EBT and some other types of public-benefits cards are an appealing target for bad actors because they largely aren't chip-enabled. Embedded microchips secure customer payments far better than magnetic stripes. The lack of chips on benefits cards make it far easier for bad actors to compromise them and "cash out." (As of early 2024, no state's EBT cards had an embedded chip, though a few states are working toward this goal.)

Additionally, some complicit retailers have facilitated the compromise and cash-outs of this card data, further exacerbating the problem.

Criminals typically cash out EBT cash benefits (those available for withdrawal at ATMs) right after these accounts receive monthly funding. This often occurs between midnight and 6 a.m. the day the benefits become available.

Criminals also often cash out Supplemental Nutritional Assistance Program (SNAP) between the first and tenth of the month. They do this through bulk purchases of readily marketable items like baby formula, energy bars and drinks, cooking oil, and candy items.

EBT cardholders generally have limited protections compared with holders of common credit and debit cards. As a result, they may not be reimbursed fully or at all for benefits lost to criminals. This, in turn, can compound their existing financial hardships. Reimbursement—when it does occur—may take weeks.

### EBT Phishing Scams

Law enforcement has also seen a significant uptick in targeted phishing, smishing, and vishing scams to compromise EBT card data.

- **Phishing** involves emails designed to get victims' personally identifiable information or financial credentials. Scammers typically pose as a creditor, bank, or state benefits agency.
- **Smishing** uses SMS text messages instead of email.
- **Vishing** uses phone calls, generally with an automated voice.

These EBT-related calls or messages will seek to trick cardholders into entering their card details without thinking. Scammers achieve this by creating a sense of distress. They often do this by referencing the closing of the EBT account or a loss of funds.

## Protect Yourself

- 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 as fully as possible when you enter your PIN to prevent cameras from recording your entry. Keep in mind that a pinhole camera may be present anywhere on or around the terminal.
- If possible, use ATMs in a well-lit, indoor location., These may still be compromised, but are less-vulnerable targets.
- Be especially alert for skimming devices in tourist areas, since these are popular targets.
- When possible, use debit and credit cards with chip technology. There are fewer devices in the U.S. that steal chip data than magnetic strip data. However, the mag-stripe data on the backs of these cards is still vulnerable.
- Avoid using your debit card when you have linked accounts, since the card's compromise will give criminals access to all of the accounts. Use a credit card instead.
- Routinely monitor your credit card, bank, and EBT or other benefits accounts to promptly identify any unauthorized transactions. If possible, set email or text-message alerts to notify you of card or account transactions.
- Proactively review the account-security options available for any payment cards you use. These options can include multi-factor authentication of transactions or freezing an account between your own transactions. Such steps may seem inconvenient, but they significantly reduce the risk of financial losses.
- Contact your financial institution immediately if the ATM doesn't return your card after you end or cancel a transaction. This may suggest the presence of a foreign device in the card reader.
- If you receive a call, text, or email asking for card information, you should separately: Contact the relevant state benefits agency to verify the authenticity of the message(s), and/or verify the status of the EBT account and current funds using a known balance inquiry line or website, or the relevant mobile application.
- If you receive a call, text message, or email asking for your PIN, never provide it. State benefits agencies won't request cardholder PINs. They'll use other means to authenticate your account.
- Always use a strong PIN. Avoid using PINs that may be easily guessed, such as strings of the same or consecutive numbers.
- If you suspect your EBT card was compromised in this type of scam: Immediately contact your state benefits agency or card issuer.
  Promptly change your PIN if any funds remain in your EBT account.
- Look into whether your account or EBT mobile application will allow you to temporarily block or freeze transactions on the account.

## News

**07.26.2024** Romanian National Sentenced for Using Debit Card Skimming Devices on ATMs to Steal Nearly $150,000 from Victims Throughout California
Christos Mavrokelos was sentenced to 18 months in prison and ordered to pay $75,000 in restitution for using counterfeit debit cards and skimming devices.

**07.11.2024** Criminals Are Targeting Bank and ATM Customers in Maryland
The FBI and our local law enforcement partners are investigating a surge of armed robberies, known as "jugging" crimes, at financial institutions in Maryland.

**04.01.2024** Romanian National Sentenced to More Than Six Years in Prison for Leading Scheme That Stole Benefits From Low-Income Families
Marius Oprea, a Romanian national, has been sentenced to 75 months in federal prison for leading a group that used illegal skimmers on ATMs to harvest data.

**02.29.2024** Five Defendants Arrested for Engaging in Sophisticated ATM Skimming Schemes Involving Theft of Account Information and PIN Numbers From Unsuspecting Bank Customers
At the federal courthouse in Brooklyn, an indictment charging defendants with fraud and aggravated identity theft was partially unsealed.

**02.20.2024** Glendale Man Sentenced for Using Credit and Debit Card Skimmers at Gas Stations to Steal Nearly $200,000 in Fresno and Southern California
Akop Dongelyan of Glendale was sentenced to 364 days in prison for conspiring to commit credit and debit card fraud.

**02.12.2024** One Sentenced, One Pleads Guilty in Two Separate Cases Involving Debit and Credit Card Skimming Schemes
Artak Vardanyan of Burbank was sentenced to 11 months in prison for conspiring to commit credit and debit card fraud.

**12.14.2023** Six Defendants Plead Guilty to Fraud Charges in Multi-Million-Dollar, Nationwide Skimming Conspiracy
Six defendants indicted for defrauding credit unions across the country have pleaded guilty to bank fraud conspiracy and identity theft charges.