State Privacy Office
August Privacy Tip

Protect Your Credit Cards from Skimmers and Shimmers

You can be a target of credit card skimming when you least expect it. One moment, you might be filling up on gas or withdrawing some cash from an ATM. You go about your day but later learn that criminals stole your card details and are racking up charges. While card technologies are improving, we must stay informed about the latest credit card scams, because scammers always look for ways to overcome security improvements. You can safeguard your finances by staying informed and taking precautions whenever you take out your cards.

What is a credit card skimmer?

A credit card skimmer is a device placed into point-of-sale devices that covertly records credit and debit card information from the magnetic stripes of swiped or inserted cards. As payment technologies become more secure, criminals evolve their card skimming techniques. The widespread adoption of EMV chip cards has shifted criminals' focus to areas where magnetic stripe transactions are still prevalent, such as ATMs, and areas that are slow to adopt EMV technology. This shift has led to the emergence of shimming technology, which targets EMV chips instead of magnetic stripes.

Modern skimmers now incorporate Bluetooth or other wireless technologies to transmit stolen data wirelessly, reducing the risk of detection. Some advanced skimmers can even capture your PIN. Gas station terminals, especially pay-at-the-pump stations, have become prime targets due to their frequent use and the lag in EMV chip reader implementation.

What happens when your card is skimmed?

When your credit or debit card information gets skimmed, scammers illegally capture your card details and use them to make unauthorized transactions, create cloned cards, commit identity theft, and, if a debit card is skimmed, drain your bank account. Cybercriminals could also gain access

to other accounts if additional personal information is compromised through data breaches or phishing.

Understanding card shimmers

Shimmers are inserted into the chip card reader slot of ATMs or point-of-sale terminals, where they intercept and record information from cards. Unlike traditional skimmers placed externally on the card reader, shimmers are inserted deeper into the device, making them harder to detect. Scammers can use information gleaned from shimmers to create counterfeit cards or make unauthorized purchases.

Types of credit card skimmers

Nowadays, criminals use several different models of card skimmers. These include:

- Overlay skimmers: These fit seamlessly over the existing card slot.
- Insert skimmers: These are hidden inside the card reader's slot.
- Insert shimmer: These fit into the slot where EMV chip cards are inserted.
- Wiretap skimmers: These intercept data transmission within the device.
- Bluetooth skimmers: These enable wireless data retrieval.
- Miniaturized skimmers: These may be concealed within or attached discreetly to the reader.

Protecting yourself against skimming and shimming

Credit card skimmers are designed to blend in with legitimate card readers, making them difficult to detect. However, you can protect yourself by both examining payment terminals and following some simple behaviors.

- Avoid sketchy pay terminals: While criminals targeting the point-of-sale terminals of large chains is not unheard of, always try to use card readers in well-let, high-traffic areas.
- Inspect card readers: Look for signs of tampering or suspicious attachments, such as loose or jiggly parts, or unusual protrusions.
- Cover the keypad: When entering your PIN, cover the keypad to prevent hidden cameras from capturing your information.
- Use chip-enabled cards: Whenever possible, use chip-enabled cards for transactions, as they offer greater security, even though shimming is a risk.

- Opt for contactless payments: When you tap your card to pay, you reduce the risk of skimming and shimming altogether.
- Monitor account activity: Regularly check your account activity and report any unauthorized transactions immediately.
- Use digital wallets: Mobile payment apps offer added security features like tokenization, but only use trusted services, like the one offered by your smartphone (such as Apple Wallet or Google Pay).
- Use credit cards over debit cards: If the worst-case scenario happens and you are a victim of card skimming, it is generally easier to dispute fraudulent charges with a credit card company than get money returned to your checking account if your debit card is compromised.

What to know about chip credit cards

Chip credit cards are safer than traditional magnetic stripe cards. They use an encrypted microchip to store and transmit cardholder data, which is more secure than the static data on magnetic stripes. When a chip card is inserted into a chip-enabled terminal, it generates a unique transaction code that cannot be reused, making it difficult for criminals to clone the card.

Chip cards often come with advanced security features like tokenization and dynamic authentication, reducing the risk of skimming attacks. While still susceptible to card-not-present fraud, the adoption of chip cards has significantly decreased instances of in-person skimming fraud.

What to know about tap-to-pay technology

Tap-to-pay, or contactless payment, uses near-field communication (NFC) to transmit encrypted payment data wirelessly from a chip in the card or smartphone to a secure payment terminal. This technology makes it extremely difficult for scammers to intercept and decode transaction data.

Although there have been isolated cases of fraudsters using NFC readers to skim card information from close proximity, security measures like transaction limits and authentication requirements help minimize this risk.

Advancements in encryption and tokenization continue to enhance the security of contactless payments, making them a safe and convenient option for consumers.

What to do if you’re a victim of card skimming or shimming

- Immediately contact your bank or credit card provider. Report unauthorized transactions and request a freeze or cancellation of the

affected card. They can guide you through disputing fraudulent charges and issuing a replacement card.
- Monitor your account activity for further suspicious transactions.
- Freeze your credit to help prevent identity theft. You can quickly unfreeze it if you need to apply for credit or a loan.
- Ensure that you're using unique, strong passwords for all accounts. Enable multi-factor authentication for all financial accounts (and, ideally, every account that allows it).

If your personal data has been compromised beyond your card details, contact relevant authorities and the credit bureaus to report potential identity theft and explore options for further protection.

Vigilance is the best protection from card skimming

You should always be vigilant about where you enter your credit or debit card, but, furthermore, you should regularly review financial statements and credit reports for signs of unauthorized activity. Always report any suspicious incidents to your bank or card issuer ASAP. Sign up for alerts or notifications from your financial institution to receive real-time updates on account activity. Stay updated about common scams and fraud schemes. Not only will you catch any possible card skimming, but regularly monitoring your financial accounts will help you stay vigilant about any possible fraud.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*