Your Guide to
Credit Card Skimming: How to Spot and Avoid Fraudulent Charges
The term "skimming," as applied to credit cards, involves stealing card account data during a legitimate transaction. It is then transferred to a duplicate card to make fraudulent purchases without the knowledge of the cardholder. Skimmers victimize cardholders and merchants alike, so it’s important that small business owners understand how it occurs, recognize the signs to watch for and know how to protect themselves and their customers from it.

As a reputable payment processing provider, we present this information about skimming to educate our clients and consumers in the hopes that they will never become victims of this particular type of credit card fraud.

**Skimming Setups**

According to the U.S. Secret Service, skimming is one of the most significant problems facing the credit card industry because it can happen whenever and wherever credit or debit cards are accepted. "When a credit card is skimmed, data on the card, including the account number, is electronically transmitted or stored. The credit card information can then be encoded onto a lost, stolen, or counterfeit credit card and used anywhere in the world," it explains.

**Credit card skimming occurs in a variety of ways, including:**

- A skimming device (card reader) is added to the front of an ATM, gas pump or other point-of-sale (POS) location and captures credit card information as the consumer attempts unsuccessfully to use the machine. Crooks have also been known to install skimmers on the doorframe where customers swipe their cards to gain access to ATMs at bank branches.
- A skimming device is added inside an ATM or other POS location and captures information during a valid transaction. This setup may also involve the use of a hidden pinhole video camera or a modified keypad overlay that captures the cardholder’s PIN (personal identification number).
- A corrupt employee (sometimes referred to as a carder) works alone or in collusion with fraudsters. The carder completes a valid sale and surreptitiously makes a second, unauthorized swipe of the card on a handheld card reader that captures the account information before returning the card to the cardholder. This technique is most common in restaurants, bars and other situations where the cardholder hands over their card to an employee who leaves their presence to run the transaction. Handheld skimmers are small enough to hide in an apron or pants pocket.

Whatever the scenario, the electronic skimming device captures account information stored on the magnetic strip on the back of the credit card. Usually the cardholder is unaware of what is happening. In fact, some accomplished carders use sleight of hand to swipe a card in the cardholder’s presence.
The thieves retrieve the information through a wireless transmission or by physically removing the skimmer. They encode the data onto counterfeit cards for in-person and online transactions or ATM withdrawals.

These illegal transactions typically go undetected until the legitimate cardholder receives their next statement. That’s why it’s critical that all cardholders carefully review their monthly credit card statements as well as their bank statements for any unauthorized charges or ATM withdrawals.

**Multimillion-Dollar “Business”**

In 2010, the Secret Service estimated skimming to be an $8-billion-a-year problem in the U.S. alone, accounting for more than 80 percent of fraud perpetrated at ATMs. A recent Mercator report also estimates U.S. card issuers’ total losses from credit and debit card fraud to be at $2.4 billion. That figure does not reflect losses borne by merchants, which most likely add up to tens of billions of dollars per year. Until EMV® becomes the standard for card acceptance, these figures are only likely to increase. In 2015, according to the FICO Card Alert Service, card compromises at ATMs were the highest ever recorded.

Credit card data theft in the U.S. is increasingly perpetrated by organized groups of thieves from other countries, according to a recent article in Consumer Reports magazine. Eastern Europe in particular has emerged as a thriving black-market for buying and selling skimming equipment and crucial personal financial data.

“Losses are comfortably in the multimillion-dollar range each year but are incredibly hard to authenticate because of the discreet position that most financial institutions take when asked to assess a loss figure,” FICO executive John Buzzard told the publication.

It also reports that banking industry data indicates that criminals are now focusing on debit cards, which enable them to get their hands on cash more quickly. “The figures reported by some U.S. banks show losses from fraudulent debit-card transactions using PINs have quintupled at stores in the past five years, and they’ve also risen sharply at ATMs, so it’s clear crooks are succeeding in getting people’s PINs, most likely through a combination of skimming and recording PINs,” notes Avivah Litan, a Gartner Research analyst specializing in fraud detection and prevention, in the Consumer Reports article.

**Ferreting out the Skimmer**

Skimming devices are easy to come by. They can be purchased inexpensively on the internet and on auction sites like eBay, but they can be difficult to detect by the untrained eye. ATM skimming devices in particular have become so sophisticated that many cardholders do not notice the fake but realistic-looking card readers that have been placed over the factory-installed card reader on the machine. Dozens if not hundreds of card accounts can be jeopardized at a busy ATM in a very short period of time until the thieves remove the device or it is identified and reported to the authorities.
“When a credit card is skimmed, data on the card, including the account number, is electronically transmitted or stored. The credit card information can then be encoded onto a lost, stolen, or counterfeit credit card and used anywhere in the world.”

Identifying a skimming device on an ATM or POS location at your business greatly increases your chances of thwarting credit card fraud for both you and your customers. The FBI, which often partners with the Secret Service to investigate skimming cases, offers the following general tips for detecting a skimming device and protecting card data at an ATM:

- Inspect the ATM, gas pump or POS 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. Newer ATMs may feature a picture of what the slot and keypad are supposed to look like, making it easier for users to identify any foreign devices that may have been attached.

- 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, which provides more restricted access for criminals looking to install skimmers.

- Be careful of ATMs in tourist areas, which are a popular target of skimmers.

- If your card isn’t returned after the ATM transaction or after you hit the “cancel” button, immediately contact the financial institution that issued the card.

If your business has a freestanding ATM kiosk or credit card terminals, inspect them regularly. Be on the lookout for electronic devices that have been added to the standard card reader or any other modification that may be apparent, including wires and cords. If you find something suspicious, alert law enforcement and have them investigate.

As an employer, you must also be vigilant for employees who may be involved in skimming or other illegal activities. Check your security footage for evidence that they are taking customers’ cards away from the checkout area where they can use a palm-sized skimming device to quickly and easily record data that they can then sell to their cohorts in crime.

As part of your skimming prevention efforts, establish transaction ground rules for your employees. These include never leaving the register area with a customer’s card, not allowing employees to keep personal items (i.e. purses and backpacks) that could hide a skimming device in the work area, and a reminder that security footage is reviewed randomly (although not necessarily the reason why).
If you discover that one of your employees is skimming, report them to the authorities immediately to avoid being implicated in their crime. Be sure to turn over any video you have of their actions.

Protect Your Small Business from Skimming
Despite your best efforts, your business can still fall prey to skimmers, fraudsters and identity thieves. If it does, you’ll want to know that you’re protected from the financial fallout of both physical and virtual data breaches.

At TSYS®, we offer you that peace of mind with our Data Breach Security Program, designed to help our customers meet the expenses associated with a suspected or actual breach of credit card data. Under the program, expenses from an actual or suspected data breach are met regardless of your business’s PCI compliance status as long as you are not involved in the breach.

Data Breach Security Program coverage includes:

- A forensic audit as required by the Payment Card Industry Data Security Standard (PCI DSS) whenever a data breach is suspected. This confirms whether a breach has actually occurred and pinpoints vulnerabilities in the system.

- Issuer-related expenses that cover card replacements costs, credit monitoring and other expenses related to a breach.

The costs of a data breach at a small business can easily escalate to the $25,000 to $50,000 range and possibly more. For most small business owners, that’s an unsustainable loss that can shut them down permanently. Why take that risk when affordable and comprehensive data breach coverage is available to cover you in the event of credit card fraud?

Talk to a TSYS representative today about our Data Breach Security Program and protect your most valuable asset — your small business.

©2017 Total System Services, Inc. TSYS® is a federally registered service mark of Total System Services, Inc. All rights reserved. EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries. TS6619a