Moneris SOLUTIONS

Protecting the POS

Answers to Your Frequently Asked Questions

What is skimming?

Skimming is the transfer of electronic data from one magnetic stripe to another for fraudulent purposes.

Why are Point-Of-Sale (POS) devices being stolen?

POS devices are stolen, tampered and returned to merchant locations with the intent to skim or capture credit and/or debit card data which is transferred to counterfeit cards.

What is a decoy?

A decoy is a device that resembles the merchant's device. A decoy may be used to replace a stolen device in attempt to provide the merchant with a false sense of security and often does not show the correct serial number. Once the tamper is complete, the fraudster returns to install the tampered device and removes the decoy.

What do the fraudsters do with card data?

The magnetic stripe card data is transferred to a counterfeit card which is used to make unauthorized purchases or to withdraw funds from cardholder bank accounts.

What is Moneris® doing to address fraud?

Moneris takes fraud seriously. We work closely with law enforcement and our industry partners, including Interac♦, Visa® and MasterCard† to provide education on fraudulent activity in attempt to reduce losses. We are leaders in the industry as a result of our fraud awareness training and the presentations on Industry Best Practices we deliver at seminars and conferences. We provide educational materials and contact information for vendors that specialize in security solutions for protecting Point-Of-Sale devices.

Who is responsible for protecting the Point-Of-Sale (POS) device?

Our merchants are responsible for protecting their POS devices. We recommend all POS devices be treated like cash.

Why should I protect my Point-Of-Sale (POS)?

By protecting the POS device, you are protecting customer card data. The negative impact on a merchant's reputation or brand (due to card compromises) can be significant and may impact the merchant's profitability.

How can I protect my Point-Of-Sale (POS)?

Moneris recommends a layered approach to fraud prevention as no single solution is sufficient to prevent fraud.

Devices can be protected by tethers (steel cable) or secure stands. In addition, we suggest the use of security seals in conjunction with a number of industry accepted best practices (e.g. daily integrity checks, audits of device serial numbers, video cameras, and employee hiring practices).

Moneris SOLUTIONS

PROTECTING THE POS

What are the benefits of using a Secure Stand, Tether and Security Seal?

Stand: The stand is secured to the counter and is locked down to keep the device in place.

Tether: The tether provides more flexibility than a stand and allows the device to be handed to a cardholder to enter their PIN and the POS to be stored under the counter, out of sight when not in use. When using a tether, the device can be easily inspected for the recommended integrity checks and serial number validation. In the event the cable is cut during the theft of a device, the fraudster is less likely to return to install the tamper as the cable will not be intact.

Security Seals: Security seals provide an added layer of security. The seals should be placed over seams (where the front and back cover meet) or over an access entry point. Any cuts through the seal or removal of the seal indicate the device may have been tampered with. Some seals also have a security feature that imprints "VOID" on the device if the seal has been removed.

What do I do when my device is stolen?

Merchants are required to immediately report the theft of a POS device to Moneris and the local authorities.

If I rent my POS devices, am I responsible for the replacement cost when it is stolen?

Yes. Please refer to the terms of the Moneris merchant agreement regarding equipment rented from Moneris.

What is the cost of a Secure Stand and Tether?

The cost of a secure stand and tether vary depending on vendor, device type and volume ordered.

Where can I purchase a Secure Stand or Tether?

A list of device security vendors is available on our website at **moneris.com**.

Will a Stand, Tether or Seal prevent my POS device from being stolen or tampered?

No security solution will completely address this issue. By protecting your POS device, you can help reduce the likelihood of fraud. We recommend a layered approach which encompasses both physical security solutions and process related best practices.

What kind of activity should I consider to be suspicious?

Some examples of suspicious activity include: individuals loitering near an unattended device, individuals placing large items on the counter to block an employee's ability to see the device or individuals that ensure they are your last customer of the day and your first customer the following morning (in some cases to return goods they have purchased). The latter technique is to steal the device at the end of the day, leave a decoy, and return the tampered device the next day.

Are there things I should look for that should cause me to suspect that my device may be tampered?

- if the serial number of the device is not part of your inventory
- if the device is no longer secure in the stand (screws missing or loose)
- if security seals are peeled back, cut or have been removed
- if the tether or cable has been cut

Moneris SOLUTIONS

PROTECTING THE POS

How can I be sure that my device has been tampered?

Only a certified technician can confirm that a device has been tampered.

What happens when my device has been tampered?

In most cases Moneris will send an investigator to your location. The investigator will gather information and evidence relating to the fraud and provide recommendations regarding potential further enhancements to device security.

Will my customers find out their debit or credit card was compromised at my place of business?

Moneris does not disclose this information (unless otherwise required to so in accordance with applicable laws), however, in some instances cardholders may talk to each other and determine the location. There have been instances of compromises reported by the media.

What is my responsibility regarding the skimming incident and the compromised cards?

The merchant is responsible for fully cooperating with Moneris (or its representative(s)) during the skimming investigation and to make every effort to prevent repeat occurrences.

Should I contact the police regarding my device theft or tamper?

Yes. A police report should be filed for a device theft or a tamper.

What should I do when someone wants to inspect, remove or perform work on my Point-of-sale device?

Only authorized persons are to perform work on your device. Moneris will always make contact with the location or the head office prior to attending the place of business. Our technicians and investigators will have Moneris identification available. Do not hesitate to telephone our contact centre to validate they are a Moneris employee.

Should I consider upgrading to a more secure device?

If you have not upgraded your Point-Of-Sale equipment to a device that can process chip cards, please contact our sales team at **1-866-421-1667** to discuss your needs. Upgrading to a new device will not prevent skimming. A layered approach to device security is your best defence against this fraudulent activity.

Are the newest POS devices being deployed by Moneris tamper proof ?

Point-Of-Sale devices are tamper resistant, not tamper proof. Devices deployed by Moneris are certified to industry standards and contain tamper resistant security features.

What best practices can I put in place to deter skimming activity?

- Educate yourself and your staff about skimming.
- Know your point of sale equipment and recognize any changes.
- Maintain care and control of your card processing equipment.
- Ensure a layered approach to point of sale devices security.
- Install video security cameras (90 days storage).
- Consider a monitored alarm system (when applicable).
- Establish good hiring practices (security, credit and reference checks).

Where can I get more information about industry best practices?

Visit **moneris.com/fraud** to review Interac's Protect Your PinPad Toolkit and download information regarding a Law Enforcement initiative called Project Protect.

Moneris SOLUTIONS

Visit **moneris.com/fraud** to review Interac's Protect Your PinPad Toolkit and download information regarding a Law Enforcement initiative called Project Protect.

Moneris SOLUTIONS