



Security <sup>TM</sup>  
Standards Council

**Standard:** PIN Transaction Security Program  
Requirements and  
PCI Data Security Standard

**Date:** August 2009

**Author:** PCI SSC PIN Transaction Security  
Working Group

## **Information Supplement: Skimming Prevention – Best Practices for Merchants**

# Table of Contents

- Chapter 1: Overview..... 3**
  - About This Document ..... 4
  - What is Card Skimming and Who Does It? ..... 4
    - Data from Consumer Payment Cards ..... 4
    - Data Capture from the Payment Infrastructure ..... 4
    - Perpetrators and Targets..... 4
  - Examples of Terminal Fraud ..... 6
- Chapter 2: Guidelines and Best Practices ..... 10**
  - Merchant Physical Location and Security ..... 10
    - Threat-Mitigating Resources ..... 10
    - Physical Protections ..... 11
  - Terminal and Terminal Infrastructure Security..... 12
    - Terminal Surroundings..... 12
    - IP Connectivity ..... 13
    - Individual Terminal Data ..... 13
    - Terminal Reviews ..... 14
    - Terminal Purchases and Updates ..... 14
    - Terminal Disposal..... 14
    - PIN Protection..... 15
    - Wireless Terminals ..... 15
  - Staff and Service Access to Payment Devices ..... 16
    - Staff as Targets ..... 16
    - Hiring and Staff Awareness..... 16
    - Outside Personnel and Service Providers ..... 17
  - Risk Analysis of Terminals and Terminal Infrastructure ..... 18
    - Identification of Assets..... 18
    - Threat and Probability..... 19
    - Severity ..... 19
    - High Transaction Volume..... 19
    - Terminals with Heavy Use ..... 19
    - High-Volume Sales Periods ..... 19
  - The Impact of Skimming Attacks ..... 20
    - Card-Issuers and Payment Networks ..... 20
    - Merchants ..... 20
    - Consumers ..... 20
- Appendix A: Risk Assessment..... 21**
  - Risk Assessment Questionnaire ..... 21
  - Risk Category..... 23
- Appendix B: Evaluation Forms..... 24**
  - Terminal Characteristics Form ..... 24
  - Merchant Evaluation Checklist ..... 25

## Chapter 1: Overview

The primary mission of the Payment Card Industry Security Standards Council (PCI SSC) is to ensure the security of payment data and the security of the payment infrastructure that processes that data. PCI SSC is committed to build trust in the payment process and payment infrastructure for the benefit of all constituents. As the threats and vulnerabilities of fraud evolve, payment constituents can and should expect the emergence of further security standards and requirements for terminal types, terminal infrastructure, payment devices, and payment process.

This document was created to assist and educate merchants regarding security best practices associated with skimming attacks. Though currently not mandated by PCI SSC, guidelines and best practices documents are produced to help educate and create awareness of challenges faced by the payment industry. The guidelines are the result of industry and law enforcement understanding of the current and evolving threat landscape associated with skimming. In addition we have incorporated known best practices, currently conducted by many merchants, to mitigate skimming attacks taking place in their respective point-of-sale environments. .

This document contains a non-exhaustive list of security guidelines that can help merchants to:

- Be aware of the risks relating to skimming.
- Be aware of the vulnerabilities inherent the use of point-of-sale terminals and terminal infrastructure.
- Be aware of the vulnerabilities associated with staff that has access to consumer payment devices.
- Prevent or deter criminal attacks against point-of-sale terminals and terminal infrastructure.
- Identify any compromised terminals as soon as possible and notify the appropriate agencies to respond and minimize the impact of a successful attack.

Additional security can—and must—be provided by merchants to enhance the security provided by the current PCI SSC standards and payment terminal vendors. Merchants have an obligation to ensure their respective payment systems and infrastructure are secure. Merchants are the first line of defense for POS fraud and are involved in the execution of the vast majority of controls suggested or required by PCI SSC. Merchants can achieve appropriate security and trust levels at the point of sale by considering all the factors that can influence overall security in their terminal environment and taking the necessary countermeasures detailed in this document to ensure an appropriate level of security.

## About This Document

This document consists of the following:

**Chapter 1** provides a general overview; describes exactly what card skimming is, who does it, and how it impacts the various payment constituents; and provides some real-life examples of compromised terminals.

**Chapter 2** provides an extensive list of best practices and guidelines merchants need to consider if they have not done so all ready. The list identifies threats and challenges and possible remedies merchants can take to mitigate the risk of being a victim of a skimming attack.

**Appendix A** provides an option for the merchant to further quantify risk associated with merchant location and terminal infrastructure.

**Appendix B** provides a checklist that merchants can use to identify and track terminal assets.

## What is Card Skimming and Who Does It?

Skimming is the unauthorized capture and transfer of payment data to another source, for fraudulent purposes. This unauthorized capture and transfer of payment data is different than mass data compromise breaches, and can result from one of two event types.

### *Data from Consumer Payment Cards*

The first type of skimming event is the acquisition of payment data directly from the consumer's payment device (payment card). This is normally accomplished through a small, portable card reader. Normally this occurs during a payment transaction conducted by the consumer at a merchant location and usually involves internal merchant personnel who have both criminal intent and direct access to the consumer payment device (payment card) with little or no observation at the time of payment. The majority of skimming attacks deal with the capture of payment data from magnetic-stripe payment cards.

### *Data Capture from the Payment Infrastructure*

The second type of skimming event results from the capture of payment data within the payment infrastructure at the merchant location, with a focus on compromised POS terminals and their respective infrastructures (terminal locations, wires, communication channels, switches, etc). Criminals will insert electronic equipment, by various means, into the terminal or the terminal infrastructure, in order to capture consumer account data. The skimming equipment can be very sophisticated, small, and difficult to identify. Often it is hidden within the terminal so neither the merchant nor the cardholder knows that the terminal has been compromised.

### *Perpetrators and Targets*

Understanding the lengths that criminals go to in order to obtain and compromise account data may help you understand the necessity of taking sufficient measures to make it significantly more difficult for the criminals to target your particular location.

#### **Who Does It?**

Regardless of how it is achieved, skimming is a highly profitable criminal activity, difficult to prevent and detect. As a result, it appeals to both ends of the criminal spectrum:

- The most sophisticated and dedicated organized criminal elements, leading to very complex and surprisingly effective attacks on the merchant terminal infrastructure; and

- The most common, least sophisticated of criminal elements, who use readily available, simple technology and direct access to consumer payment cards.

Criminals want a high and rapid rate of return, regardless of the type of theft they are considering. Skimming allows them to capture massive amounts of account details in a short amount of time, with low risk of detection. As a result, it often is their first and foremost consideration.

## Targets

### *PIN Data*

In addition to the acquisition of account data on the card, criminals are very interested in the acquisition of PIN data. The industry and law enforcement have seen significant efforts to acquire PINs at the payment terminal by the following means, among others:

- “Shoulder-surfing” by individuals stationed nearby the POS device
- Placement of fake PIN entry devices (PEDs), ATMs, or readers and CCTV cameras directed at the PED on the payment terminal

### *Unattended or Temporarily Unmanned Terminals*

Merchant locations that for a wide variety of justifiable business needs have self-service terminals, unattended payment terminals, exterior payment terminals, and/or multiple terminal locations not manned all the time, for all shifts, are prime targets for intrusive terminal and terminal infrastructure attacks.

Criminals will also target large multi-lane retailers where, during less busy periods, not all of the lanes are used and terminals are effectively left unattended. Criminals will steal terminals, compromise them, and then return them to either the same store or to another store in the same chain.

## Examples of Terminal Fraud

The following photographs are designed to assist in understanding the attack techniques used by criminals at merchant locations.

Photograph	Attack Technique
	<p>Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically.</p> <p>As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number.</p> <p>Additionally, run your finger along the label to check that it is not hiding a compromise.</p>
	<p>Terminals often have security stickers, or company stickers placed over screw holes or seams that will act as indicators if the case has been opened.</p> <p>Criminals often remove these labels when compromising terminals and may replace them with their own printed versions.</p> <p>When you first receive the terminal, make careful note of label position, color, and materials used.</p> <p>Also look for any signs that the label may have been removed or tampered with.</p>

Photograph	Attack Technique
------------	------------------



Skimming devices hidden within the terminal will not be visible and neither the merchant staff nor the cardholder will know that the card has been skimmed.

This picture shows a skimming device inserted in a terminal. This would have been hidden by the SIM card cover plate.



Key loggers are used to record all keystrokes made, in this case by an electronic cash register.

Key loggers can be very small and can look like part of the normal cabling. It is therefore essential to pay close attention to detail when performing any inspection.



Changes to terminal connections can be difficult to spot.

In these images, the criminals completely changed the cable used to connect the terminal to the base unit.



This was to incorporate the additional wires required to capture card data.

Photograph	Attack Technique
	<p>The modern digital cameras used to record the cardholder entering his or her PIN are very small when removed from their case.</p> <p>This makes them very easy to hide or disguise at the merchant location.</p> <p>This type of miniature camera can easily be hidden in a ceiling tile above the terminal.</p>
	<p>Staff should also be aware of additional, unfamiliar electronic equipment connected to the terminal, the cash register, or the network connections.</p> <p>This device records and decrypts ISDN data.</p>
	<p>Handheld skimmers used by corrupt staff are very small, fitting in the palm of your hand.</p> <p>Despite their size, these devices can store a significant amount of account details.</p>
	<p>In this picture, the criminal entered the merchant location posing as a service engineer.</p> <p>He stated that to prevent credit card fraud the terminal must be placed in this secure box. He then gave the staff a sheet of printed instructions.</p> <p>The box contained a card skimmer and miniature camera.</p> <p><b>Be cautious of unannounced service visits.</b></p>

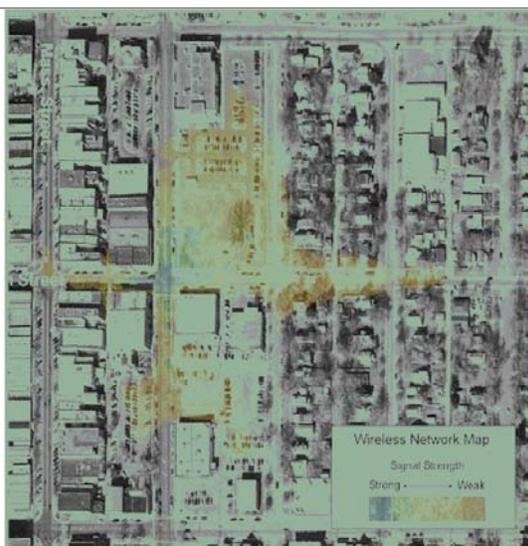
**Photograph**

**Attack Technique**



These devices were used to connect into the telephone exchange of a shopping mall to record all transmissions from the stores to the merchant's financial institution.

Such devices usually consist of voice recorders or MP3 players with very large memories. Often they have external batteries for improved life.



This aerial view clearly shows how Wi-Fi signals can extend far beyond the four walls of the merchant location.

## Chapter 2: Guidelines and Best Practices

Best practices and security guidelines for the prevention of skimming are based on successfully established countermeasures as identified by the merchant community, and known criminal activity as observed and investigated by the payment industry and law enforcement.

Guidelines and best practices fall within three major areas.

- **Merchant Physical Location and Security:** Many merchants have realized the benefits of operational and physical security countermeasures that not only provide a consistent brand image and transparent consumer experience, but also have the necessary physical security and operational controls required to support their retail locations and POS environment.
- **Terminals and Terminal Infrastructure Security:** Leveraging PCI SSC standards and approved devices should be considered a core component of any terminal security effort. Merchants should make every effort to leverage and use the controls, standards, and devices, already established by PCI SSC for the protection of devices and data at the point of sale. The guidelines and recommended practices we provide complement those standards.
- **Staff and Service Access to Payment Devices:** Employee and staff conduct should be a critical concern to all merchants, specifically in the processing of payment data and services.

### Merchant Physical Location and Security

The merchant's physical location, nature of business, and payment terminal structure has a significant impact on the likelihood of being targeted by criminal organizations for skimming. Merchants select and operate their business locations based on a wide variety of business conditions and requirements. These include but are not limited to the type of business a merchant has, the brand image they wish to project, the type of customer they seek, the cost to operate a facility, the ability to access and maintain an employee base, the ability to get consumer throughput based on retail location, and security and environmental issues required for the business.

A merchant's physical location, once selected, must rely on physical security and operational controls to maintain a safe and secure environment for their employees, customers, and their line of business. The need to conduct a formal security risk analysis to identify risks, both logical/systems-based risk analysis and physical/operational-based risk analysis, for the business is critical to a merchant's overall operation and success.

Relative to physical location and business type, a merchant's ability to mitigate terminal and terminal infrastructure attacks is based primarily on the extent of the physical security and security operations (monitoring) that can be supported by the business.

#### *Threat-Mitigating Resources*

Merchants are encouraged to use every possible resource they have available to mitigate the threat. This would include but not be limited to:

- The use of physical security systems;
- Physical security structure and design techniques for the pos and the retail space in general;
- Security operational processes;

- Terminal checklists and procedures;
- The use of terminal and payment equipment which adheres to PCI SSC standards; and
- The use of security consultants and security services (guard operations).

### *Physical Protections*

Some best practices suggested for terminal and terminal infrastructure relative to site location and business type include the following:

#### **Terminals**

- Design payment locations with the additional intent to control customer access to payment technology and the payment location. Designs should include the protection and security of equipment and the respective cables and power sources. Security should extend into the ceiling and below flooring levels of the payment location, when applicable.
- Leverage and use vendor controls for terminal equipment and payment devices to their fullest extent possible.
- Leverage current DSS and PCI SSC standards and practices for terminals, terminal infrastructure, and the payment data they process. Also look to the new device standards for the protection of PIN data using approved POS PED, EPP, and UPT devices.
- Secure all terminals to the physical structure of the payment location when possible. (See “Terminal Security and Terminal Infrastructure Security” below). Place payment terminals and technology in a manner that offers the greatest level of security (less consumer and employee access), observation, and monitoring when possible.
- Physically secure and alarm all remote or self-service terminal payment environments to the greatest extent possible. Use long-standing retail physical security concepts (facility and site lighting, facility and site access, physical security systems, security operations and checks, etc.) to complement payment locations and support terminal security needs. Focus specifically on unattended terminals and payment locations to prevent skimming attacks.

#### **Terminal Infrastructure**

- Secure terminal wiring and communication lines with conduit or within physical structures of the facility when allowed or required by local building codes. Limit exposed terminal cable and wire or non-secure channels for communication infrastructure when possible. The intent should be to make it as difficult to access terminal wiring and cabling as possible, requiring more time on site to tamper or compromise terminal cabling.
- Protect all telephone rooms, panels, routers, drops, and connections that support terminal infrastructure. Use locks and control access to sensitive electrical and telephone closets that support payment infrastructure. Conduct regular checks of this infrastructure as required with management and security staff trained to be on the lookout for compromises.

## Cameras, Placement, Access, and Image Storage

### Note:

*PCI SSC recommends that duty staff do not have direct unencumbered access to surveillance cameras, recording and control equipment, or tapes. Management or security personnel should review recordings on a recurring basis or when required to support an incident.*

- Use applicable lighting to support payment environments and CCTV monitoring capabilities as required. Ensure ATMs are well lighted and meet minimum physical requirements as defined by the appropriate regulatory mandates.
- The surveillance cameras should be sited such that they record the area around the POS PED device, without actually being capable of recording any PIN number entered.
- Support PCI SSC guidelines for 90-day storage of CCTV images.
- Locate cameras to cover primary site entrances and facility entrances. Use CCTV to monitor payment lanes and locations when possible. Facility cameras provide a level of deterrence and a record of activity that can be used to support investigations.
- Immediately examine all terminals if a camera has been moved, damaged, or if images have been blocked. This may be an indicator that criminals have targeted your merchant location.
- Note the following:
  - Time stamps – in case the camera was switched off for a period of time.
  - Any blackouts.
  - Any period when the CCTV image is blocked.
  - Any incidence when the camera is moved.

## Terminal and Terminal Infrastructure Security

It is very important to fully understand the security implications of your terminal environment. Where you choose to locate your terminal(s) – and everything that surrounds the terminal – has an impact on how easy it is for a criminal to compromise that terminal.

Terminals and terminal infrastructure are a major investment for the merchant and should be included in any site or location security risk analysis program. They support the lifeblood of any business, the actual payment process.

Improvements in terminal security require significantly more time for a criminal to compromise the terminal. PCI SSC has recently developed new security standards for payment terminals that support POS PED, EPP and UPT (Unattended Payment Terminals). However, due to the range, age, and type of terminals in use in the market today, criminals can still target merchant locations with older and “weaker” terminals or terminal infrastructure.

### Terminal Surroundings

Once you have secured the terminal in its location, you need to be aware of its immediate surroundings and how this can be used to provide criminals with an opportunity to compromise cardholder data. Modern terminals offer a wide range of connectivity methods to enhance the ease and speed of transactions for the cardholder. Merchants should be aware that certain parts of the transaction data are transmitted in clear text format. Because criminals can target this data, it is essential that all staff understand and record all connections to the terminal and note the entire cable path from the terminal to the point where it leaves your merchant location. It is not unusual for criminals to replace a cable or to insert logging equipment at any point in the path between the terminal and the external connection point at the merchant location. This could allow

a criminal to eavesdrop on the terminal's communication, regardless of the method you use to transmit card data to either your host or your head office.

## IP Connectivity



### Warning!

- *Do NOT drill into terminals to connect cables, as this triggers security mechanisms inside the terminals, which will cause them to stop working.*
- *Criminals will often try to steal a terminal to allow them more time to compromise it, and will later return it.*
- If terminal connections use shared wire with other merchant business applications in the retail facility, note any impact to other applications and remember to include a review of terminals and payment technology accordingly.
- Secure terminal cabling in public areas with conduit, or within physical structures where possible. The intent should be to make it as difficult to identify and access payment terminal wiring and cabling as possible, requiring more time on site for a criminal to tamper with it.
- Do not identify or tag the cable as terminal cable in your facility. If tagging is required, develop a code that limits easy identification of the cable as a payment terminal cable.
- ➔ Consider cable locks: Some terminals have slots so that you can attach a cable lock (as used to secure laptop computers) to the terminal. This can then be threaded through the cable connecting the terminal to the cash register and then secured to prevent both the terminal and the cable from being compromised. **This is strongly recommended as a best practice.** To insert a skimming device, it is often necessary to remove the terminal from its location, or swap the existing terminal for another compromised terminal.

## Individual Terminal Data

An essential step in protecting your terminals is to record the number, type, and location of each of your terminals. Such details will allow you to easily determine whether you have been targeted. See Appendix B for an example checklist on how to track and manage this data. For each terminal:

- Record its make, model, and serial number.
- Record its location in the store (unless the terminals are removed and secured when the store is closed).
- Record the condition and location of any labels.
- Record the exact details of any security labels.
- For PIN pads and POS PED devices connected to an electronic cash register, or separate host system, record how the terminal is connected.
- Record how many connections (leads, plugs, aerials, etc.) are normally associated with each terminal. Record the style, type, and color of each connector, or take a photograph to show the number and the type of connectors used.
- Mark each terminal with an ultra-violet (UV) security pen to provide a unique identifier for that terminal,

**Additionally:**

- Use the security standards for POS PED and UPT to support your overall terminal security program.
- Replace older terminals (weaker terminals) with approved PCI SSC terminals.

**Terminal Reviews**

Use the sample forms in Appendix B to track and monitor terminal assets. Ensure these are reviewed on an ongoing basis by merchant or security staff.

- ➔ Build these terminal reviews into your shift changes, security guard tours of your facility, and/or when a terminal service call is initiated. Make it habit and a daily procedure to document and monitor your terminal environment, and train your staff to the importance of terminal and terminal infrastructure security.

*PCI SSC strongly recommends that you purchase terminals either directly from the vendor, or through a legitimate and recognized distributor. Although there are companies that offer refurbished terminals for sale, merchants must be cautious when using these suppliers to ensure that they fully understand the history of the terminals and can confirm with the vendor the security and integrity of any terminals purchased.*

**Terminal Purchases and Updates**

It may be necessary at certain points throughout the lifetime of the terminal to update the software of the terminal, or import new keys. Any process that involves changes to the terminal introduces increased risks. Before commencing any changes, modifications, or updates, ensure that you obtain the correct authorizations, and that only legitimate personnel are involved in the process.

When performing updates, especially the loading of new keys, it is essential that you:

- Maintain dual control at all stages.
- Complete and retain proper logs and control sheets.

When purchasing new terminals, make sure they have been approved and meet the requirements of the PCI PTS Security Evaluation Program and the DSS. Check the particular model numbers, including the hardware revision and firmware revision, to ensure that the model is compliant.

Refer to [www.pcisecuritystandards.org/pin](http://www.pcisecuritystandards.org/pin) for a list of all PCI-approved terminals.

**Terminal Disposal**

Merchants need to dispose of old terminals in a secure and consistent manner. Some items to consider:

- Return old terminals to authorized dealers via secure shipping or direct pick-up when new terminals are installed. This may make business sense for the merchant, in addition to providing a secure manner to dispose of old terminals.
- Clear terminal operating system and application data from all memory when possible. Check with the terminal manufacturer to help determine requirements.
- Remove all tags and store or business identifiers.
- If possible, develop a contract with an authorized vendor who can help dispose of electronic materials and components in a secure and environmentally friendly manner.
- If possible, do not dispose of terminals in trash containers or dumpsters associated with your store, for the obvious reasons.

## ***PIN Protection***

As well as capturing the Track 2 data containing details of the cardholder's account number, the criminals will also wish to obtain the PIN to maximize the compromise. The PIN, once entered, is encrypted throughout the data chain so the criminal must either compromise the terminal to allow PIN capture during entry, or—more commonly—insert a miniature camera to observe and record the PIN as it is entered.

Digital technology has enabled cameras to become significantly smaller. Criminals can hide the devices in numerous ingenious ways, so their presence may not be obvious to staff or customers. Criminals have been known to hide cameras in:

- False ceilings above PIN Pads
- Boxes used to hold leaflets
- Charity boxes next to PIN Pads

Understanding how and where criminals can hide cameras helps to reduce such threats. While the area around a cash desk is a prime location for merchandise, it is essential that stands containing goods, leaflets, or even charity boxes must not be situated next to, or near,

PIN Pads or POS terminals. Train staff to be aware of any changes to the area around the till, especially any new boxes that appear, which could house a covert camera.

As part of the ongoing check of your merchant location, staff should also pay close attention to the ceiling area, especially where there is a false ceiling. It is very difficult to spot the very small hole required for the camera, so look for the more obvious signs of entry or change, such as a tile that has been lifted, moved, or handled. Refer to Chapter 1, “Examples of Terminal Fraud,” for a visual example.

## ***Wireless Terminals***

Modern payment terminals can offer various methods of wireless connectivity. This may enable those merchants without access to a dedicated telephone network, the capability of accepting debit and credit transactions, or to provide a better service to cardholders.

Wireless connectivity allows the terminal to be removed from the cash desk, such as in a restaurant where the terminal can be taken to a table to allow the customer to pay their bill without losing sight of their payment card.

While this offers benefits to the cardholder and further limits the exposure to employee skimming activity, the risk to the merchant is that it is very easy for a criminal to steal such a terminal, modify it, and return it without anyone realizing it has gone.

- ➔ *It is therefore essential that you know how many terminals are in use each day, and devise a method to identify quickly who has the terminal at any particular time. For example, you could give each staff member a token, which they must leave at the cash desk whenever they take the terminal away.*

The types of terminals mentioned above are usually either “Bluetooth” or “Wi-Fi” enabled. You must be aware that, although designed to operate over short ranges, criminals can intercept Bluetooth and Wi-Fi signals over significant distances, and certainly beyond the walls of your merchant location. (See “Examples of Terminal Fraud” in Chapter 1.) It is therefore essential that you enable all proper security functions on the terminal and, where necessary, apply all security updates and patches.

These terminals connect to their host system via the GPRS (mobile phone) network. This allows merchants who are not at fixed locations, such as music concerts or festivals, to accept credit and debit card payments. As there is no fixed location, it is you, the merchant, who is responsible for ensuring the integrity and security of the terminal and that you store it securely when it is not in use.

## Staff and Service Access to Payment Devices

To talk about staff in relation to criminal activity is a very sensitive topic. Naturally most employers consider their staff to be loyal, hardworking, and trustworthy. But that trust needs to be validated and established at the time of hire, and then proven over time by appropriate behavior. We need to recognize that all businesses need to measure an employee's level of responsibility and protect access to sensitive data and payments on an on going basis.

It is important to be aware that employees may have a criminal background at the time of hire or develop criminal intent over their time of employment. Internal fraud committed by staff is a very difficult subject to address but we need to recognize it can be the most insidious and damaging type of theft that a business encounters. Unfortunately, it is a fact that employees hired into certain business types have conducted skimming.

### *Staff as Targets*

Staff members maybe considered prime targets for criminals using either bribery or coercion, especially in high-risk merchants where the number of staff on duty at any one time is limited. Criminals may offer up to a year's salary to a sales assistant to "look the other way", or even to help with skimming cards. They may also target the employee's family in order to coerce the employee to carry out its fraudulent work. Therefore:

- Your company must have a specific policy covering these issues to allow staff to report any kind of inappropriate approach to them by criminals.
- Staff must be able to report to senior management anonymously, as it has been known for criminals to target store managers.
- Train your staff to be aware of the types of fraud attacks criminals may attempt and the risk to them. The staff needs to understand the necessity of completing regular terminal and terminal infrastructure checks, and learn how to spot any changes that could indicate that an attack has taken place.

### *Hiring and Staff Awareness*

When hiring new staff, the merchant should always conduct a background check where allowed by law. These background checks help protect the merchant and the consumer and allow the merchant to make an informed decision on an applicant at the time of hire.

- Background checks could and should include validation of employee data as supplied in the hiring process, a criminal check, a financial/credit check, and an education check. Previous employment history should also be in scope when applicable. This is the best way to validate a new employee's statements and ensure you are hiring the best possible candidate.

If background checks are not allowed by law, or not available, then the merchant should at least have the following data on the employee:

- Full name
- Full address and telephone number
- Date of birth
- Photo
- Previous work history
- References
- National ID, Social Security Number, etc.

It is essential to train all new staff to ensure that they know how to protect the terminal environment by being aware of what to look out for.

In addition all staff should understand the notification and escalation process to report an event:

- The procedure for escalating concerns about a terminal.
- Who to contact if they have concerns about terminal security.
- How to contact senior management if they discover a compromise.
- How management or the employee should contact local law enforcement if someone threatens or attempts to bribe them to compromise terminals or payment data.

### ***Outside Personnel and Service Providers***

In addition, there are personnel that support payment terminals or terminal infrastructure not directly controlled by the merchant. These personnel can range from terminal service technicians, security officers, facility maintenance personnel, telephone personnel, mall staff, etc. Though not directly controlled or managed by the merchant, merchants can indicate the type of service and behavior they want on their premises and in the service of their equipment. Insist on background checks for these personnel from your service providers. Communicate how you want incidents reported to you when discovered by these personnel.

- Service level agreements can and should be leveraged by the merchant to get additional checks and controls from these service providers for terminal checks, terminal infrastructure support, and physical security controls when applicable.
- If it becomes necessary to call a service engineer, you must clearly agree to a time, date, and if possible confirm the name of the service engineer who is to conduct the service.
- If a service engineer, or someone purporting to be a service engineer, arrives at your merchant location unannounced, then you must not allow any access to any terminals until you have verified that person's credentials. This must include contacting the vendor, or service company, to confirm their identity.
- All work undertaken by the service engineer must be written down in a report, which is retained for at least six months.

## Risk Analysis of Terminals and Terminal Infrastructure

*Appendix A provides an example of a risk analysis questionnaire that could be used by merchants to assess their terminal and terminal infrastructure.*

In addition to the guidelines, PCI SSC recommends merchants seek out and use qualified security professionals and consultants to help them assess risk at their retail locations and terminal environments. Because of the variety and types of merchant POS environments in the marketplace, merchants can come to different conclusions of exactly how best to implement mitigating controls for skimming attacks, using the guidelines below as a baseline.

A risk analysis process for skimming attacks and the POS, at a minimum, should include the identification of assets, the identification of threats, and the probability of the threat's taking place. This in turn should lead to the identification of those countermeasures and controls that best mitigate the threat at a specific merchant location and POS environment.

### **Identification of Assets**

The identification of assets is a critical first step to any risk analysis process. In this case we are focused on the terminal and terminal infrastructure. In the section marked "Terminal and Terminal Infrastructure Security" we have indicated the level of detail required to have a very clear understanding of your terminal environment. Asset identification would include the number of terminals, their location and surroundings, the number of ports, asset identification tags, wire or cable identification, routers, cabling, etc.

## ***Threat and Probability***

We have spoken in detail on the extent of the threat associated with skimming and its impact to all constituents in the payment channel. What we have not discussed is probability of the threat. Probability is based on likelihood that a skimming incident will take place at your location. We have identified the fact skimming takes place at an ongoing, recurring, daily basis. It is one of the three most common threats or fraud types the payment industry deals with, and we believe at least dozens of events take place on a daily basis, globally. We have also discussed the concept of location and business type that attract skimming interests, which raises the vulnerability of any given merchant to this attack.

## ***Severity***

The other concept that merchants should be aware of is the severity of a skimming attack. This can be qualified by the number of accounts compromised and the dollar loss associated with any given card compromised within the skimming attack. Hundreds of cards can be compromised very quickly within a skimming attack, with average losses ranging at few hundred US dollars per card. Skimming attacks in total can range from a few thousand to millions of dollars. This does not include the other types of costs associated with the skimming event, such as customer notification and card replacement, merchant remediation, fines, etc.

There have been many cases where criminals have:

- Stolen terminals from cash lanes and desks not in use,
- Broken into a store and taken only the terminals,
- Broken into a store and compromised the terminals,
- Hidden themselves in the store until it closed and compromised the terminals overnight, leaving when the store re-opened, or
- Swapped a good terminal for a compromised terminal, using large items to block attendants' line of sight.

## ***High Transaction Volume***

Merchants with a high volume of payment transactions are also at risk. For the criminal, the intent is to get as much account and PIN data as possible in the shortest amount of time. Merchants fitting this risk profile normally have significant numbers of payment transactions for smaller dollar amounts. Petrol stations are an example of both unattended terminal risk and high payment volumes, making them prime targets for skimming activity. Other merchant locations and or business types also fit this profile.

## ***Terminals with Heavy Use***

A single payment terminal used for a large number of transactions may attract criminal intent. (In-store ATMs are a good example, or where relatively few terminals support a business.) The idea is to capture as many accounts as simply and quickly as possible—it's more efficient to compromise one terminal with high activity than to attack three terminals with the same volume of accounts.

## ***High-Volume Sales Periods***

As you develop operational business and security controls for peak activity, keep in mind that criminals also target merchants during busy sales times, whether they be holidays or special events. Again, the intent is to capture as many accounts and PINs in as short a time as possible.

## The Impact of Skimming Attacks

The impact of skimming is significant for all the constituents involved in payment services. Skimming attacks undermine the integrity of the payment system and process, employee trust, industry relationships, and consumer trust and behavior in merchants. There is a cost to skimming attacks that is over and above the actual loss of monies, goods, and services.

### *Card-Issuers and Payment Networks*

For banks and the various sources of funding for payment cards, the issue is direct financial loss and loss of trust in the payment system. The cost of the fraud itself, incremental monitoring requirements, investigative efforts, consumer notification efforts, and the cost to replace cards are just some of the issues associated with a skimming incident for the issuing banks and payment networks.

### *Merchants*

For the merchant, recent attacks in the headlines have led to realization that a single fraud incident can put merchants out of business or at the very least significantly impact their brand and the trust people have in them. Skimming fraud is one of the top three fraud types a merchant must address. Consumers are becoming more aware of which merchants protect their information and which ones do not and are taking their business to different locations or merchants and modifying their choice of payment type accordingly. Any move back to historical payment types (checks, cash, etc.) should be seen as a troublesome and costly trend for merchants. A merchant has the additional challenge and cost of dealing with a skimming event to include the cost of forensics and system analysis, system upgrades based on recommendations, industry fines, lawsuits, employee terminations, loss of goodwill, and other liability concerns.

### *Consumers*

The loss of consumer trust in their payment brand and the payment system is not good for anyone involved in the payment chain. Not only must the consumer deal with the inconvenience of their compromised account data but they are also challenged to return to their normal payment practices after such an event. This loss of trust is leading to strained relationships between merchants, merchant-servicing financial institutions, and the various payment networks. Some observed consumer behaviors after a skimming incident are very disconcerting for both financial institutions and merchants. They include but are not limited to changes in buying patterns, changes to shopping locations, self-reduction of credit lines, movement to alternate payment methods and their respective cost management (cash), and less use of direct debit card products at the point of sale (specifically when a PINs are also compromised).

## Appendix A: Risk Assessment

This Appendix enables you to determine the risk category that applies to your particular merchant location.

Complete the following questionnaire to determine a “vulnerability score,” and therefore the risk category applicable to your merchant premises. For each question, there are two or more possible answers, each of which has a particular value. For each question, enter the relevant value under “Your Score.”

### Risk Assessment Questionnaire

No.	Question	Finding	Value	Your Score
1	Where are your merchant premises located?	Town center	1	
		Shopping mall	1	
		Out of town	2	
2	Are your merchant premises isolated?	Yes	1	
		No	0	
3	If the answer to question 1 is “Out of town” and to question 2 is “No,” how many shops or businesses are in the same location as your premises?	1 – 3	3	
		4 – 10	2	
		> 10	1	
4	Are your premises located at, or near, a major highway?	Yes	1	
		No	0	
5	Are your merchant premises open ...	24 hours	2	
		Extended hours	2	
		9 – 5 (or similar)	1	
6	How many days per week are your premises open?	7	2	
		6 or less	1	
		Seasonal	2	
7	During public holidays, are your merchant premises ...	Open	1	
		Closed	0	
8	Do your premises have CCTV that is recorded?	Yes	0	
		No	1	
9	Do staff have access to the CCTV and the recorded data?	Yes	1	
		No	0	
10	Whilst your premises are open, how many staff are on duty?	< 3	3	
		4 – 10	2	
		> 10	1	
11	During opening hours, do your premises have a duty manager working on site?	Yes	0	
		No	2	

No.	Question	Finding	Value	Your Score
12	Are your staff ...	Skilled	0	
		Semi-skilled	1	
		Unskilled	2	
13	Do you employ seasonal staff?	Yes	1	
		No	0	
14	Do you employ casual staff?	Yes	1	
		No	0	
15	Do you have a high turnover of staff (>20 per year)?	Yes	1	
		No	0	
16	When your business is closed, are contract cleaners allowed onto the premises?	Yes	1	
		No	0	
17	If the answer to question 16 is "Yes," are the cleaners escorted?	Yes	0	
		No	1	
18	Do you use a hybrid or "slide-and-park" reader for chip card transactions?	Yes	1	
		No	0	
19	Do you have checkout desks that are not used during normal business hours?	Yes	1	
		No	0	
20	When not in use, do your POS PED devices remain at the checkout desk?	Yes	1	
		No	0	
21	Are checkout desks that are not in use monitored and recorded by CCTV?	Yes	0	
		No	1	
22	Do your premises have a high, regular, or low throughput of customers per day, or do you have peak periods at certain times of the day?	High	3	
		Regular	1	
		Low	1	
		Peak periods	2	
23	Are there particular days in the week when you are very busy?	Yes	1	
		No	0	
24	Are there special times throughout the year when you are particularly busy?	Yes	1	
		No	0	
25	If you open during public holidays, are these particularly busy days for you?	Yes	1	
		No	0	
26	Has your business been approved to PCI Data Security Standards?	Yes	0	
		No	1	
		Don't know	1	

No.	Question	Finding	Value	Your Score
27	Are all your terminals PCI POS PED approved?	Yes	0	
		No	1	
		Don't know	1	
28	Have your premises already been the subject of a payment card fraud attack?	Yes	1	
		No	0	
		Don't know	1	
29	Have your premises been burgled within the last six months?	Yes	1	
		No	0	
<b>TOTAL SCORE:</b>				

## Risk Category

When you have answered all questions, total the scores in the right-hand column to determine your overall vulnerability score and therefore your risk category.

Vulnerability Score	Risk Category
More than 25	High risk
17–25	Medium risk
16 or less	Low risk

## Appendix B: Evaluation Forms

This Appendix provides sample forms that you can use to verify the integrity of your terminals and terminal environment.

### Terminal Characteristics Form

Complete one copy of this form (or similar) for each terminal (PIN entry device or PIN pad) used at your location.

Terminal Description	
<b>Location:</b>	<b>Location when not in use:</b>
<b>Make:</b>	<b>Model Number:</b>
Terminal Details	
Serial number (on printed label):	
Serial number (on screen, if applicable):	
General condition and appearance (color, existing marks, scratches, etc.):	
Location of manufacturer's security seals or labels:	
Details of manufacturer's security markings or reference numbers:	
Details of any UV markings applied to the terminal:	
How is this terminal connected to its host device?	
<ul style="list-style-type: none"> <li>• Connection #1: Connector type, color of lead:</li> <li>• Connection #2: Connector type, color of lead:</li> <li>• Connection #3: Connector type, color of lead:</li> <li>• Connection #4: Connector type, color of lead:</li> </ul>	
How many connections in total (all leads, plugs, aerials, etc)?	
Describe any display stands, charity boxes, or other merchandising materials that are normally placed within the vicinity of this terminal.	
Describe the "normal" condition of the ceiling above the terminal (include scuffmarks, fingerprints, dislodged tiles, etc.).	

## Merchant Evaluation Checklist

Complete a copy of this checklist (or similar) each time you evaluate your terminals and terminal environment. (This form assumes there are five terminals deployed, T1–T5.)

With reference to the relevant Terminal Characteristics Form, for each terminal:	T1	T2	T3	T4	T5
Is the terminal in its usual location?	Yes or No				
Is the manufacturer's name correct?	Yes or No				
Is the model number correct?	Yes or No				
Is the serial number printed on the label correct?	Yes or No				
Is the serial number displayed on screen correct?	Yes or No				
Is the color and general condition of the terminal as described, with no additional marks or scratches (especially around the seams)?	Yes or No				
Are the manufacturer's security seals and labels present, with no signs of peeling or tampering?	Yes or No				
Are the manufacturer's security markings and reference numbers as described?	Yes or No				
Are any expected ultra-violet markings present, and as described?	Yes or No				
Are all connections to the terminal as described, using the same type and color of cables, and with no loose wires or broken connectors?	Yes or No				
Count the number of connections to the terminal. Does this agree with the number stated?	Yes or No				
Are all display stands, charity boxes, or other merchandising within the vicinity of this terminal as described, with no additional boxes or display materials near to the terminal?	Yes or No				
Is the condition of the ceiling above the terminal the same as described, with no additional marks, fingerprints, or holes?	Yes or No				
Is the total number of terminals in use the same as the number of terminals officially installed?	Yes or No				
Where surveillance cameras are used, is the total number of cameras in use the same as the number of cameras officially installed?	Yes or No				