



Information about this New Document

New document	This <i>Security Guidelines for Merchants' Terminals</i> , dated August 2008 is an entirely new document.
Contents	This document contains a non-exhaustive list of security guidelines relating to the use of Point-of-Sale terminals at merchant locations.
Billing	MasterCard will not bill principal members for this document.

Using this Document

Legal Disclaimer The MasterCard *Security Guidelines for Merchants' Terminals* is not an exhaustive or complete set of guidelines, and MasterCard reserves the right to modify this material or provide additional and other guidelines at any time in its sole discretion.

No party should rely upon this document as an assurance of quality, reliability, and security, and MasterCard specifically disclaims any and all representations in connection with the materials contained in this document. MasterCard International shall not be liable for and specifically disclaims responsibility for any party's infringement of any intellectual property right arising out of the use of this document.

Purpose The MasterCard *Security Guidelines for Merchants' Terminals* aims to help merchants understand the risks relating to the use of Point-of-Sale terminals and to monitor, maintain, and improve the security of their terminal environment.

Audience MasterCard provides this document for members and their authorized agents. Specifically, the following personnel should find this document useful:

- Acquirers and their merchants
- Terminal vendors

Times Expressed

MasterCard is a global company with locations in many time zones. The MasterCard operations and business centers are in the United States. The operations center is in St. Louis, Missouri, and the business center is in Purchase, New York.

For operational purposes, MasterCard refers to time frames in this document as either “St. Louis time” or “New York time.” Coordinated Universal Time (UTC) is the basis for measuring time throughout the world. You can use the following table to convert any time used in this document into the correct time in another zone.

	St. Louis, Missouri, USA Central Time	Purchase, New York, USA Eastern Time	UTC
Standard time	09:00	10:00	15:00
(first Sunday in November to second Sunday in March ¹)			
Daylight saving time	09:00	10:00	14:00
(second Sunday in March to first Sunday in November ²)			

Excerpted Text

At times, this document may include text excerpted from another document. A note before the repeated text always identifies the source document. In such cases, we include the repeated text solely for the reader’s convenience. The original text in the source document always takes legal precedence.

Language Use

The spelling of English words in this document follows the convention used for U.S. English as defined in *Merriam-Webster’s Collegiate Dictionary*. MasterCard is incorporated in the United States and publishes in the United States. Therefore, this publication uses U.S. English spelling and grammar rules.

An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

1 For Central European Time, last Sunday in October to last Sunday in March.
2 For Central European Time, last Sunday in March to last Sunday in October.

Revisions

MasterCard periodically may issue revisions to this document to accommodate enhancements and changes, or as corrections are required.

With each revision, a Summary of Changes describes how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The date of the revision appears at the right of each revision marker.

MasterCard may publish revisions to this document in a MasterCard bulletin, another MasterCard publication, or on MasterCard OnLine®. A subsequent revision is effective as of the date indicated in that publication or on MasterCard OnLine and has precedence over any previous edition. In the event of a conflict between this document and a subsequently published edition, the subsequently published edition shall have precedence.

Organization

The following table provides an overview of this document.

Part	Description
Chapter 1, Introduction to Card Fraud	Introduces the problems related to card fraud and provides some real-life examples of compromised terminals.
Chapter 2, Risk Assessment	Discusses the risks associated with particular types of merchant.
Chapter 3, Security Guidelines	Discusses the risks associated with the use of payment terminals and provides security 'best practices' that help to mitigate those risks.
Chapter 4, Merchant Evaluation	Describes a methodology to verify the integrity of terminals and the terminal environment.
Appendix A, Risk Assessment Questionnaire	Helps determine the risk category that applies to a particular merchant location.
Appendix B, Evaluation Forms	Provides sample forms to use to verify the integrity of terminals and the terminal environment.

Related Information The following documents and resources provide information related to the subjects discussed in this document:

- *POS Terminal Security Program – Approval List*
- *Security Guidance for Card Acceptance Devices Deployed in the Face to Face Environment*, David Baker, APACS, February 2007
- *Merchant Education Tool Kit*, Interac Association, April 2007

For information relating to the MasterCard POS Terminal Security Program, and the PCI Merchant Education Program, refer to www.MasterCardMerchant.com.

For information relating to the Payment Card Industry POS PED Security Requirements and the PCI Data Security Standards, refer to www.pcisecuritystandards.org.

Additional resources and information will also be available from your acquirer and from your local Payment Association.

Definitions of key terms used in this document are available in the *MasterCard Dictionary*.

To order MasterCard documents, please use the Ordering Publications tool, available in the Quick Links section on the Member Publications home page, or contact the Customer Operations Services team.

Contact Us

MasterCard is listening...

Please take a moment to provide MasterCard with your feedback about the *Security Guidelines for Merchants' Terminals*.

MasterCard continually strives to improve user documents. User feedback helps MasterCard accomplish this goal.

Please provide feedback about this document to Manuals and Publications at publications@mastercard.com.

Support

Please address your questions about MasterCard programs and services to the Customer Operations Services team as follows.

Phone:

1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

Fax:

1-636-722-7192

Telex:

434800 *answerback*: 434800 ITAC UI

Address:

MasterCard Worldwide
Customer Operations Services
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

E-mail:

Canada, Caribbean, Latin America, and United States customer_support@mastercard.com

Asia/Pacific:

Australia and New Zealand csd@mastercard.com

China, Hong Kong, and Taiwan helpdesk.gc@mastercard.com

Southeast Asia helpdesk.singapore@mastercard.com

Japan/Guam opetokyo@mastercard.com

Korea korea_helpdesk@mastercard.com

Europe and South Asia/Middle East/Africa css@mastercard.com

Spanish language support lagroup@mastercard.com

Vendor Relations, all regions vendor.program@mastercard.com

Contacting Your U.S. Member Relations Representative

Member Relations representatives assist U.S. members with marketing inquiries. They interpret member requests and requirements, analyze them, and if approved, monitor their progress through the various MasterCard departments. This does not cover support for day-to-day operational problems, which the Customer Operations Services team addresses.

For the name of your U.S. Member Relations representative, contact your local Member Relations office:

1-678-459-9000 Atlanta

1-847-375-4000 Chicago

1-924-249-2000 Purchase

1-925-866-7700 San Francisco

Contacting Your Regional Representative

The regional representatives work out of the regional offices. Their role is to serve as intermediaries between the members and other departments in MasterCard. Members can inquire and receive responses in their own languages and during their offices' hours of operation.

For the name of the location of the regional office serving your area, call the Customer Operations Services team.



Security Guidelines for Merchants' Terminals

August 2008

Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available:

- On MasterCard OnLine®
 - On the *MasterCard Electronic Library* (CD-ROM)
-

Address

MasterCard Worldwide
2200 MasterCard Boulevard
O’Fallon MO 63368-7263
USA

www.mastercard.com

Chapter 1 Introduction to Card Fraud.....	1-i
Overview	1-1
What is Card Skimming?	1-2
How Does this Affect Me?.....	1-2
Examples of Terminal Fraud.....	1-3
Chapter 2 Risk Assessment.....	2-i
Introduction	2-1
Throughput.....	2-1
Location	2-2
Staffing.....	2-2
Opening Hours.....	2-2
Size and Type of Premises.....	2-3
Connectivity of the Terminal	2-3
Risk Assessment.....	2-4
Understanding the Results of your Risk Assessment.....	2-4
High Risk Merchant	2-4
Medium Risk Merchant	2-5
Low Risk Merchant	2-5
Chapter 3 Security Guidelines	3-i
Introduction	3-1
Security Best Practices	3-1
Physical Location	3-2
Terminal Environment	3-2
Staff.....	3-5
New Staff	3-5
Surveillance Cameras.....	3-6
Service Personnel.....	3-7
Terminal Connectivity	3-7
Data Security.....	3-9
Purchase of New Terminals	3-9
Visual Guide	3-10
Chapter 4 Merchant Evaluation	4-i
Introduction.....	4-1
When to Conduct an Evaluation.....	4-2
Terminal Characteristics Form.....	4-2
Merchant Evaluation Form.....	4-4
Conducting an Evaluation.....	4-4

Table of Contents

Appendix A Risk Assessment QuestionnaireA-i
Risk Assessment.....A-1

Appendix B Evaluation Forms B-i
Terminal Characteristics Form.....B-1
Merchant Evaluation Checklist.....B-2

Chapter 1 Introduction to Card Fraud

This chapter introduces the problems related to card fraud and provides some real-life examples of compromised terminals.

Overview 1-1

What is Card Skimming? 1-2

 How Does this Affect Me?..... 1-2

Examples of Terminal Fraud..... 1-3

Overview

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

- Be aware of the risks relating to the use of Point-of-Sale (POS) terminals.
- Prevent or deter criminal attacks against POS terminals used at their location.
- Identify any compromised terminals as soon as possible in order to minimize the impact of a successful attack.

MasterCard takes great care to ensure that the security of new POS PIN Entry Device (POS PED) products meets the highest standards. However, it is not sufficient to rely solely on this security to protect cardholders' details from being defrauded at merchant locations.

Additional security can – and must – be provided by merchants to enhance the security provided by the terminal itself. You can achieve this by considering all the factors that can influence overall security and taking the necessary countermeasures detailed in this document to ensure a high level of security for cardholders using your merchant facility.

This document contains four chapters and two appendices. This chapter provides a general overview, describes exactly what 'card skimming' is, and provides some real-life examples of compromised terminals.

[Chapter 2, Risk Assessment](#) deals with assessing risk and describes how you can determine the risks relevant to your particular location. [Appendix A, Risk Assessment Questionnaire](#) provides a related Risk Assessment Questionnaire that will enable you to determine how vulnerable you are to potential attacks. Completing the Risk Assessment Questionnaire is an essential first step in protecting your POS terminals and cardholders from fraud.

Understanding the risk that your merchant location will be targeted by criminals is a vitally important first step. Once you understand this risk then you can evaluate your location and implement the necessary steps to reduce this risk and best protect your terminals.

[Chapter 3, Security Guidelines](#) describes the factors that make a merchant location a target for criminals and discusses how each of these factors can affect overall security. This chapter provides 'best practice' security guidelines that, once implemented, can help to reduce the likelihood of an attack, or ensure that any successful attack is discovered as quickly as possible.

[Chapter 4, Merchant Evaluation](#) describes a methodology for evaluating your terminals (and terminal environment) in order to verify that your terminals have not been subjected to an attack. [Appendix B, Evaluation Forms](#) contains sample forms to use when performing such an evaluation.

One of the common findings from cardholders, merchants, and the Police is that the first they knew that criminals had targeted a particular location was when the fraud appeared on the cardholders statement. Criminal gangs are very clever at disguising the fact that they have attacked a terminal. It is therefore essential to pay very close attention to the smallest details when checking your terminals.

The main goal of the criminal organizations that are behind the majority of fraud attacks against POS PED terminals is to obtain as many credit or debit card account numbers as they can, including the PIN if at all possible. This enables them to defraud cardholder's accounts by withdrawing cash anywhere in the world. Such fraud nets substantial amounts of money for the criminal gangs.

As a result, the criminal organizations have significant resources available to fund attacks against modern terminals in order to implant skimming devices or bugs. Where this is not possible then they invest heavily in alternative methods of capturing cardholder details.

Offset against this is the prospect of either being caught, or the compromised terminal being discovered and removed. Criminals rely on the fact that merchants generally focus their attention on running their businesses and do not consider themselves targets for attack. By implementing the guidelines and procedures described in this document, the criminals will be much less likely to succeed if they target your location.

What is Card Skimming?

'Skimming' is the transfer of electronic data from a customer's credit or debit card to another source, for fraudulent purposes. Depending on which country you live in, your customers may use either a chip card or a magnetic stripe card, some of which require the cardholder to sign a sales voucher to confirm the sale, while others require the customer to enter their PIN at the terminal.

Criminals will try to insert electronic equipment into the terminal, or intercept the data communication path, in order to capture card data. If successful, this enables them to create false cards with which to perform fraudulent transactions.

The skimming equipment can be very small and difficult to identify. Often it is hidden within the terminal so that neither the merchant nor the cardholder knows that the terminal has been compromised.

In addition, criminals may insert a very small digital camera in or around the terminal to record the PIN as the cardholder enters it on the terminal's keypad.



How Does this Affect Me?

Credit and debit card fraud affects all the parties in the payment chain. It is important that cardholders feel comfortable using their credit or debit cards to pay for the goods or services you provide. Cardholders learn very quickly the whereabouts of merchants who have been compromised, and will either avoid using your location, favor you competitors, or use cash instead of their cards.

This document will enable you, the merchant, to follow best security practices to deter criminals from compromising your terminals and defrauding cards at your location, and thus protecting your business.




Examples of Terminal Fraud


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

	<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 with the electronic serial number. If they do not match then contact your acquirer or MasterCard.</p> <p>You should also check by running your finger along the label that a compromise is not being hidden by the label.</p>
	<p>Terminals often have security stickers, or company stickers placed over screw holes or seams that will detect if the case has been opened.</p> <p>When you first receive the terminal make careful note of the position, color, and materials used. Criminals can remove these labels when compromising terminals and may replace the label with their own printed version.</p> <p>Also look for any signs that the label may have been removed or tampered with.</p>

Introduction to Card Fraud

Examples of Terminal Fraud

	<p>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.</p> <p>This picture shows a skimming device inserted in a terminal. This would have been hidden by the SIM card cover plate.</p>
	<p>Key loggers are used to record all key strokes made, in this case by an electronic cash register. They can be very small and can look like part of the normal cabling.</p> <p>It is therefore essential to pay close attention to detail when performing any inspection.</p>
	<p>Changes to the connections of the terminal can be difficult to spot.</p> <p>In these images, the criminals completely changed the cable used to connect the terminal to the base unit.</p> <p>This was to incorporate the additional wires required to capture card data.</p>

	<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 unknown electronic equipment which is connected to either the terminal, or 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>These devices can still store significant numbers of card details.</p>

Introduction to Card Fraud

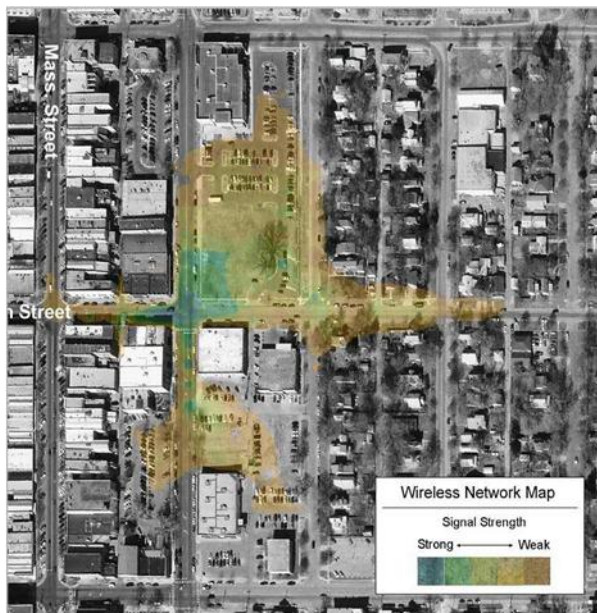
Examples of Terminal Fraud



In this picture, the criminal entered the merchant location posing as a service engineer. 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. The box contained a card skimmer and miniature camera. Be cautious of unannounced service visits.



These devices were used to connect into the telephone exchange of a shopping mall to record all traffic from the stores to the acquirer. They 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 way beyond the four walls of the merchant location.

Chapter 2 Risk Assessment

This chapter discusses the risks associated with particular types of merchant.

- Introduction 2-1
 - Throughput..... 2-1
 - Location 2-2
 - Staffing..... 2-2
 - Opening Hours 2-2
 - Size and Type of Premises..... 2-3
 - Connectivity of the Terminal 2-3
- Risk Assessment..... 2-4
 - Understanding the Results of your Risk Assessment..... 2-4
 - High Risk Merchant 2-4
 - Medium Risk Merchant 2-5
 - Low Risk Merchant 2-5

Introduction

By understanding the likelihood that your POS PED terminals are targets for criminal attack significantly helps you, the merchant, to adopt the best preventative measures to avoid such attacks.

It is important to avoid introducing radical, strict, time-consuming measures for locations that are unlikely to be targeted, as they quickly become ineffective. However, ignoring the risk of attack enables criminal gangs to target you, with significant impact on the cardholders using your merchant location – your customers!

Experience in a significant number of fraud cases around the world has found that there are a number of factors which affect the likelihood of a particular merchant location being targeted for fraud. The key risk factors are:

- Throughput of cardholders
- Location
- Staffing levels, including susceptibility of staff to bribery or coercion
- Opening hours
- Size and type of merchant
- Connectivity of terminals

As with most situations, there is not one key factor that affects the criminals' choice of a particular location but a number of factors that, when added together, result in your particular location being at a higher or a lower risk of attack.

Throughput

Criminal gangs are always looking for a quick return. They tend to target a particular location for a short period, typically 2–3 days, with a week generally being the maximum. This is based upon several factors:

- The chance of the compromise being discovered
- The number of cardholder details the skimming equipment is capable of storing
- The battery life of the equipment used (if a battery is used)
- Whether bribery or coercion of staff is required

Therefore, criminals want a location that has a high throughput of cardholders and, preferably, with a limited number of terminals to reduce the chance of cardholders using a terminal that has not been compromised.

The best situation for the criminal is when the merchant location is very busy at certain times of the day and very quiet at others. This is especially necessary for merchant locations open 24 hours a day.

Location

The actual citing of your premises also influences the criminal's decision about whether or not to target a particular location. The two main factors that increase the risk are:

- If you are in an isolated location – particularly if it is on, or near, main roads or junctions.
- If you are located in an out-of-town retail park, in an area with a limited number of other merchants.

There is also an increased risk if you are located near areas where there are significant numbers of holidaymakers, or visitors from other countries.

Staffing

Staffing levels have a direct impact on the risk of your location becoming a target. Put simply, the fewer staff you have working at your location at any given time, the more likely you are to be targeted for attack.

If your location has less than three members of staff working together then there is an increased risk. The highest risk is if there is only one person working at a merchant location during certain periods of the day.

Experience has shown that criminals often attempt either to bribe staff, (with bribe levels approximately equal to one year's wages being offered), or use coercion, against both the member of staff and his immediate family.

This risk is increased if the staff member has access to CCTV recording equipment, as they can switch off the equipment whilst the compromise is occurring so there is no visual record of the criminal performing the attack.

Another area of risk associated with staff is their loyalty towards the company. Historically, staff were thought of as the first line of defense against the criminal trying to compromise a terminal. However, with different types of employment opportunities, different working patterns, and different wage structures, traditional staff loyalty cannot be guaranteed – or even expected.

Opening Hours

The risk associated with opening hours falls into three main categories:

- Stores that close for a period
- Stores that are open 24 hours a day
- Stores that only open for a particular season

This risk is linked to the opportunities available to the criminal to compromise one or more terminals.

When stores close for a period (for example, overnight, or on certain days of the week) the criminal has the opportunity to break into the premises to compromise the terminals and insert miniature cameras to observe PIN entry. It is not unusual for a store to be broken into and there be no signs of anything being taken. However, having to break into a merchant location does increase the risk to the criminal of being caught, as they may set off an alarm.

Stores that stay open for extended hours, or 24 hours a day, and where there is a limited number of staff on duty, provide the criminal with the opportunity to swap a terminal, insert a camera, or both, without being noticed. This is especially true if your facility has:

- Numerous checkout desks or lanes, where some lanes are used only at busier times of the day
- Checkout desks spread out around the store where some are used only during busy periods

Those stores that open only for a particular season provide a significant opportunity for the criminals to compromise the terminal out of season. This is likely to occur just before the location opens for trading at the start of the new season.

Size and Type of Premises

There are different risks associated with the size and type of the premises:

- Small stores in busy locations, with a limited number of terminals, limited staff numbers, and that open long hours, are at greater risk of being targeted by criminals.
- Larger stores, especially out of town DIY stores or garden centers, where there are scattered pay points, many of which are used only at certain times of the day or week, give ample opportunities for criminals to swap out a terminal and or insert hidden cameras to capture PIN entry. It is also possible for criminals to hide in a large store unnoticed until the store closes, when they have time to compromise the terminals before returning to hide until the store re-opens – and then they can simply walk out.
- Large stores in shopping malls present a different risk, associated with the routing of the connection between the terminal and the host. For large shopping malls, criminals have been known to target the telephone exchange and insert wire-tapping devices to capture the data as it is sent from the merchant location.

Connectivity of the Terminal

Today's modern terminals offer many different methods of connectivity. Historically terminals connected to the acquirer host (or processor) by a dial-up telephone line. Today there are other alternative methods available, including:

- IP connectivity
- Wi-Fi
- Bluetooth
- GPRS

These different methods of connectivity present their own risks. The biggest risk (compared to traditional terminals) is that wireless signals can travel through walls and ceilings and be monitored and captured in the street and in adjacent buildings. It is essential that, when purchasing or leasing a wireless terminal, it fully complies with the MasterCard POS Terminal Security (PTS) requirements and has been 'PTS-approved'.

When using IP connectivity, it is important that you adopt the best practices of the scheme in terms of data handling and storage, and ensure that your location has been evaluated against the requirements of PCI Data Security Standard.

Risk Assessment

Everyone suffers when criminals attack a merchant. It is therefore essential that, for every merchant location, a thorough risk assessment is performed to assess the likelihood of that location being the target of a criminal attack.

To assist in this process, use the questionnaire in [Appendix A, Risk Assessment Questionnaire](#) to identify your **risk category**. This will then determine the actions you need to implement to mitigate the risk of attack.

Understanding the Results of your Risk Assessment

The aim of the Risk Assessment Questionnaire is to identify how likely your merchant premises are to being targeted by criminals for attack. In this document, merchant locations are categorized as **High Risk**, **Medium Risk**, or **Low Risk**.

Understanding that different merchants have different risks will help you to focus your efforts to prevent or defeat an attack.

High Risk Merchant

Being a high risk merchant does not automatically mean that criminals will target you immediately. It does, however, highlight the fact that merchants similar to you **have** been targeted, and it is possible that you also will be targeted. It is therefore essential that you verify the integrity of your terminals and terminal environment on a **daily** basis.

Knowing that you are a high-risk target can enable you to be on guard against attack. Think like an organized criminal and ask yourself these questions:

- When are the busy periods both during a day and throughout a week?
- Are public holidays very busy periods for me?
- Are there certain times of the year (such as summer holidays, winter skiing, etc.) that are particularly busy periods for me?

Remember that the criminal wants to target a merchant for the shortest period and to generate the maximum number of credit or debit card details. Therefore, just before these busy periods could well be when the criminal would target your premises.

Medium Risk Merchant

As a medium-risk merchant the chances of being targeted are obviously less than for those in the high-risk category. However, this does not mean that you are not a potential target. Therefore, it is essential that you verify the integrity of your terminals and terminal environment on a **weekly** basis.

You need to understand when your busy periods are, so that you can be at your most vigilant in the days leading up to them. The problem that you face as a medium-risk merchant is that the vast majority of such merchants will not be targeted, and continuing to perform regular checks that continually find nothing may be a challenge. Therefore, it is essential that these checks become routine and that they form a regular part of the working day or working week. Regular re-training of staff is essential to ensure that they are aware of the risks and what it is they are trying to protect.

Low Risk Merchant

As a low-risk merchant, it is unlikely – though not impossible – that you will be targeted for attack by criminal gangs. However, this does not mean that it could not happen, and so you should verify the integrity of your terminals and terminal environment on a **monthly** basis.

As with medium-risk merchants, the main problem is that your regular checks may find nothing unusual and that on a weekly, monthly, and possibly even a yearly basis, you may not be a target. Again, it is essential to ensure regular re-training of staff, to reiterate the threat, and what the protections are designed to achieve.

By regularly verifying the integrity of your terminals and terminal environment, you remain in a good position to discover or prevent an attack.

Chapter 3 Security Guidelines

This chapter discusses the risks associated with the use of payment terminals and provides security 'best practices' that help to mitigate those risks.

Introduction	3-1
Security Best Practices	3-1
Physical Location	3-2
Terminal Environment	3-2
Staff.....	3-5
New Staff	3-5
Surveillance Cameras	3-6
Service Personnel.....	3-7
Terminal Connectivity	3-7
Wireless Connectivity.....	3-8
Bluetooth and Wi-Fi Enabled Terminals	3-8
GPRS Enabled Terminals	3-8
Data Security.....	3-9
Purchase of New Terminals	3-9
Visual Guide	3-10

Introduction

This chapter describes ‘best practice’ in the form of a non-exhaustive set of security guidelines, designed to help you to mitigate the risks associated with your terminal environment.

After reading these guidelines, we recommend that you perform a Risk Assessment of your facility to understand into which **risk category** your location falls. This information can then be used to provide the best support for your terminals and the best defense against fraudulent attack.

We also recommend that you follow the procedures described in [Chapter 4, Merchant Evaluation](#) to record the details of each POS PED device used at your location, and regularly use a checklist to verify the integrity of your terminals and terminal environment.

There is rarely one obvious reason for a criminal to target a particular merchant location – typically, it is a combination of several of the key factors. When reading these guidelines, you should therefore consider all of the key factors when deciding how best to protect your location from attack.

It is important to point out that we are dealing with organized criminal gangs, who have access to significant resources and the very latest equipment, enabling them to mount very sophisticated attacks against your merchant location. These criminal organizations consider compromising terminals and obtaining credit and debit card details to obtain cash as their ‘normal’ job. They want maximum return for minimum risk so it is up to you, the merchant, to help prevent attacks from happening by using the information provided in this document.

A criminal organization targeting a particularly busy merchant location has been known to obtain sufficient card details to cause in excess of USD 1M of fraud from one terminal. Knowing this scale of potential reward should help you to understand the necessity for implementing the security best practices described in this document.

Security Best Practices

This section provides ‘best practice’ security guidelines relating to your:

- Physical location
- Terminal environment
- Staff
- Surveillance cameras
- Service personnel
- Terminal connectivity
- Data security
- Purchase of new terminals

Physical Location

Your physical location has a significant impact on the likelihood of you being targeted by criminal organizations. As mentioned, these organizations want a high return, in terms of the number of credit and debit card details captured, in the shortest time, and with as low a risk as possible of being caught, or of the compromise being detected.

Criminals will target isolated merchant locations situated near, or at, busy junctions to major highways, and especially those locations that are open extended hours, with very few staff on duty during those hours. Obvious targets in this category would be petrol stations.

A second key target is out-of-town stores such as garden centers, or DIY stores, especially those that open extended hours or are particularly busy at certain periods (for example, public holidays).

Finally, criminals may target a shopping mall to gain access to the telephone communications system using wire tapping, rather than targeting an individual store.

Obviously, as a merchant your location cannot be changed, so it is important to understand the risks associated with your particular physical location and implement all other guidelines to protect yourself from attack.

Terminal Environment

It is very important to fully understand the security implications of your terminal environment.

Where you choose to site your terminal(s) – and everything that surrounds the terminal – has an impact on how easy it is for a criminal to compromise that terminal.

Improvements in terminal security have resulted in it taking significantly more time for a criminal to compromise the terminal. However, due to the range, age, and type of terminals in use, criminals can still target merchant locations with older and ‘weaker’ terminals.

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. Therefore, if your terminal is located at, or near the entrance to your store you may wish to consider providing additional security to prevent the terminal from being removed, such as locking it in a stand which is permanently attached to a cash desk or sales counter.

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.

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

It is important to consider how vulnerable your terminals are when they are not in use. If a cash drawer left inside an unused cash till was robbed, the loss from that drawer may be around USD 200. However, if a terminal is left unattended when a lane or cash desk is not in use, the loss from that terminal may be more like USD 1M. Therefore, MasterCard strongly recommends that when they are not in use, or when the store is closed, you remove those POS PED terminals and PIN Pads and store them in a secure location.

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 in situ
- Hidden themselves in the store until it closed and then compromised the terminals overnight, leaving when the store re-opens
- Swapped a good terminal for a compromised terminal whilst covering their activity with large items of shopping

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

WARNING!

Criminals will often try to steal a terminal to allow them more time to compromise it, and will later return it.

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. For each terminal:

- Record the make, model, and serial number of the terminal.
- Record the location of the terminal in the store (unless the terminals are removed and secured when the store is closed).
- Record the state 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 connected to the 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.

Refer to [Chapter 4, Merchant Evaluation](#) for further details on how you might do this.

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 the criminals with an opportunity to compromise cardholder data.

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. Whilst 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 sited 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 a daily or weekly 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.

Staff

To talk about staff in relation to criminal activity is a very sensitive topic. Whilst we all consider our staff to be loyal, hardworking, and trustworthy, it is important to be aware that they are at risk from organized criminal gangs.

Staff members are 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 are limited. Criminals may offer up to a year's salary to a lone 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 member of staff 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. Staff must be able to report to senior management anonymously as it has been known for criminals to target store managers.

It is essential to maintain accurate records of staff attendance, including any last minute changes, and keep these records for at least six months.

Train your staff to be aware of the types of fraud attacks criminals may attempt and the risk to them; this is critical for high-risk merchants. The staff need to understand the necessity of completing regular checks, and learn how to spot any changes that could indicate that an attack has taken place. Although the chances of being targeted are less for medium and low risk merchants, performing regular checks remains critical.

For high-risk merchants, performing regular checks of all terminals and the surrounding environment must become part of the daily routine.

New Staff

When hiring new staff, always obtain the following information for each staff member including, where possible, proof of:

- Full name
- Full address and telephone number
- Date of birth
- Nationality
- Previous work history
- References

A formal application form must be completed for the post. Be cautious of any member of staff who:

- Only wants to work night shifts
- Provides only a mobile phone number
- Does not provide a permanent address
- Has changed addresses several times in recent years
- Has only recently immigrated to your country

If your merchant location has a limited number of staff (that is, less than three), then it is essential that they each provide proof of identity in the form of a government-issued document (ID card, passport, driver's license, etc). If this is not possible, take a photo of the employee and keep it on record.

WARNING!

You should be cautious if:

- **New or potential staff members provide only a mobile phone number**
 - **New staff members only want to work night shifts**
 - **Employees seem scared to answer questions, appear nervous, or who do not want to conduct, or allow, regular checks of terminals**
-

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

- The procedure for escalating concerns about a terminal
- Who to contact if they have concerns about terminal security
- How to contact local law enforcement if they discover a compromise
- Who and how to contact local law enforcement if someone threatens or attempts to bribe them

Train staff to be aware of being distracted, especially if this entails turning their back on the terminal. It takes very little time to remove or swap a terminal. Also, make staff aware of current trends in criminal attack so they are best prepared to protect your merchant location.

Surveillance Cameras

Surveillance cameras do provide a deterrent to criminals targeting a particular location. Where they are used, it is essential to record the images and keep the recordings for at least one week. We recommend that duty staff do not have access to surveillance cameras, recording and control equipment, or tapes. This is to protect them against bribery or from being coerced to switch off or remove cameras. 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.

We recommend that:

- The site manager reviews the recording each day to check for signs of criminal activity.
- Note should be taken of:
 - Time stamps – in case the camera was switched off for a period of time
 - Any blackouts
 - Any period when the image is blocked
 - Any incidence when the camera is moved
 - Any other suspicious footage
- You immediately examine all of your 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.

Service Personnel

If it becomes necessary to call a service engineer to a particular terminal, you must clearly agree a time, date, and if possible confirm the name of the service engineer who is to attend.

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.

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, you should 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

Terminal Connectivity

Modern terminals offer a wide range of connectivity methods to enhance the ease and speed of transactions for the cardholder.

You should be aware that certain parts of the transaction data are transmitted in clear text format. This data can be targeted by the criminals so 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 to your head office.

Many terminals are connected directly to their host via the Internet. This ‘IP connectivity’ enables transactions to be performed much quicker as you do not need to wait while the terminal dials up to make the connection. Also, Internet data transfer speeds are significantly quicker. However, like every computer connected to the Internet, such terminals are at risk of attack and compromise from malware, Internet attack, or computer virus. You must therefore ensure that any terminals you deploy that have Internet connectivity, or use any form of Wireless communications, have been evaluated under the MasterCard POS Terminal Security (PTS) Program and are ‘MasterCard PTS approved’. Refer to the *POS Terminal Security Program – Approval List* for a list of all PTS-approved terminals.

Wireless Connectivity

Modern payment terminals can offer various methods of wireless connectivity to 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.

Whilst this offers benefits to the cardholder, 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.

Bluetooth and Wi-Fi Enabled Terminals

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. It is therefore essential that you enable all proper security functions on the terminal and, where necessary, apply all security updates and patches.

GPRS Enabled Terminals

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.

Data Security

Cyber crime is growing in both diversity and sophistication, and criminals are increasingly targeting merchant systems in an attempt to obtain credit and debit card details.

It is essential that you fully understand how your systems work, and all the possible points in the chain where data could be stored.

In many cases, MasterCard has found that merchants are not aware that sensitive data was being stored in their systems. Therefore, merchants must adopt and follow the Payment Card Industry *Data Security Standard* process and requirements.

As a merchant, you should closely investigate your systems and networks so you can clearly identify how data flows from the point-of-interaction to the host system, paying particular attention to where data is, or could be, stored along the way. This includes where data is transferred from one server or system to the next.

Where data is stored, you must verify that the data is either encrypted or stored securely to prevent unauthorized access, and that it is only stored for the minimum time necessary.

NOTE

MasterCard does not permit the storage or track data or CVC2 data.

Purchase of New Terminals

When purchasing new terminals, make sure they have been approved and meet the requirements of the PCI POS PED Security Evaluation Program and (for Internet and wireless terminals) the MasterCard POS Terminal Security Program. Check the particular model number, including the hardware revision and firmware revision to ensure that it is a compliant model.

Refer to www.pcisecuritystandards.org/pin for a list of all PCI-approved terminals. See also the *POS Terminal Security Program – Approval List* for a list of PTS-approved terminals.

We strongly recommend 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.

WARNING!

MasterCard does not recommend purchasing second-hand terminals from Internet auction sites such as e-Bay, or other locations where the authenticity and security of the product cannot be guaranteed.

Visual Guide

When performing an evaluation of your merchant location we recommend that you use the pictures provided in [Chapter 1, Introduction to Card Fraud](#) to help identify possible risks at your location.

In addition, we recommend that you take a set of photographs of the terminals used at your location, and the environment around each terminal, so that you can quickly identify any changes.

Chapter 4 Merchant Evaluation

This chapter describes a methodology that will allow you easily to verify the integrity of your terminals and terminal environment.

Introduction	4-1
When to Conduct an Evaluation	4-2
Terminal Characteristics Form.....	4-2
Merchant Evaluation Form.....	4-4
Conducting an Evaluation.....	4-4

Introduction

Having carried out a risk assessment and identified whether your merchant location is in the high, medium, or low risk category, we recommend that you conduct an initial audit of all of your terminals, their characteristics, and the environments within which they are used. The information you gather will provide important reference information for subsequent checks, and enable you quickly to identify small details that may indicate that you have been targeted by criminals.

Refer to [Appendix B, Evaluation Forms](#) for examples of forms you can use to help you record relevant information and conduct subsequent checks. These are:

- **Terminals Characteristics Form** – Use this form to record all of the correct details of each terminal you use to perform credit and debit card transactions. Your terminals may be either stand-alone POS PED terminals, or PIN Pads connected to an Electronic Cash Register. Complete one form for each terminal or PIN Pad.
- **Merchant Evaluation Form** – Use this form to record the results of your subsequent checks, with reference to the details recorded on the relevant Terminal Characteristics Forms. Complete a copy of this form each time you evaluate your terminals and terminal environment.

The aim of completing a Merchant Evaluation Form on a regular basis is to verify that nothing about your terminals, or the environment in which they are used, has changed since the previous evaluation.

The Merchant Evaluation Form should only take a short time to complete but it is **essential that staff pay particular attention to small detail**, as this may be the only clue that something has changed. Taking pictures of the terminal, its connections, seals, markings, and surrounding area, will help identify any changes that may indicate an attack.

WARNING!

Any anomalies, discrepancies, or concerns must be reported immediately to a supervisor or manager.

The employee performing the evaluation should sign and date the evaluation form. You should store completed forms for at least six months.

When to Conduct an Evaluation

It is highly recommended that you evaluate your terminals and terminal environment as often as required according to the results of your Risk Assessment:

- Merchants that are considered **high risk** should complete a Merchant Evaluation Form **every day**.
- Merchants that are considered **medium risk** should complete a Merchant Evaluation Form **once per week**.
- Merchants that are considered **low risk** should complete a Merchant Evaluation Form **once per month**.

Criminals will often strike during the night or when the store is closed. It is therefore essential to complete the Merchant Evaluation Form first thing before the store opens for business. For stores open 24 hours a day, this can be performed at the start of the morning shift.

In addition to completing the Merchant Evaluation Form according to your risk category (daily, weekly, or monthly), you should also look at those periods in any week, month, or year, when you will be particularly busy. We recommend that you complete a Merchant Evaluation Form immediately before, and immediately after such busy periods.

For example, for a garden centre that will be very busy during a particular public holiday, in addition to the regular checks, you should perform an evaluation the day before (or the morning of) the public holiday, as this is a period when the risk of being targeted is increased.

If, as a medium-risk merchant you have a particular day each week when you are busy, then it is highly recommended that you perform an evaluation either the day before, or the morning of, that busy day.

If your merchant location is closed for a particular period (for example, a Sunday or public holiday) then it is recommended that you perform an evaluation on the first morning of opening after the closure. This is especially true for merchants who are only open for a particular season.

In addition, all staff should be encouraged to raise concerns at any time with regard to anything related to the POS PED terminal, PIN Pad or its surrounding area. If a member of staff is not happy with the explanation given for a change, he or she must have a method of reporting this concern to a higher level than the local manager.

Terminal Characteristics Form

It is recommended that you create a form on which to record the essential characteristics of each of your terminals. As a minimum, the form should capture the following information:

Terminal Details:

- The manufacturer's name and model number

- The serial number of each terminal
- The normal location of the terminal, a) when in use, and b) when not in use
- The general appearance of the terminal, in terms of color, marks, scratches etc.
- The location of any seals and security labels, and details of the manufacturer's security markings
- Details of any UV-visible security markings you have applied to the terminal to create a unique identifier for that terminal
- For PIN Pads and POS PED devices connected to a Electronic Cash Register, or separate host system, details of how each terminal is connected to the point-of-sale device
- The style, type, and color of the connector(s) used
- How many connections (leads, plugs, aerials, etc.) are connected to the terminal

Terminal Environment:

- Note the area around the terminal and record the presence of any display stands, charity boxes, etc. that are normally placed near the terminal.
- Look at the ceiling above the PED, (especially if this is a false ceiling) and record the condition of the ceiling tiles or panels. For example, do they look clean, are any fingerprints or other marks visible, and is each tile correctly positioned?

General

- The total number of terminals deployed at your location
- Where security cameras are used, the number cameras in use and the position of each

When you change or upgrade a terminal – especially when you add additional terminals – it is essential that the new or revised details are added to the form, especially manufacturer's name, model number, serial number, and details of any UV security marks you apply.

When you make changes to the sales area around the terminal (for example, you introduce new display stands that could be used to hide a camera), then once again the form must be updated.

You may consider taking photographs of the underside of the terminal to show details of the labels attached, and photographs of the surrounding sales area to show the location of display stands and other merchandising materials. Attach any photographs to the form, as appropriate.

Refer to [Appendix B, Evaluation Forms](#) for a sample Terminal Characteristics Form.

Merchant Evaluation Form

The Merchant Evaluation Form is simply a checklist you use to verify the presence, condition, and operating environment of your terminals. It is important that the form is easy to understand and simple to complete, requiring just ticks in boxes to indicate that each check has been completed. The date and time of the evaluation, together with the name of the person conducting the evaluation should also be recorded.

It is recommended that you create a form similar to that shown in [Appendix B, Evaluation Forms](#), as a series of questions that members of staff can use to check each terminal for any small changes to the terminal itself, and to the environment in which it is used.

Include a column for each terminal so that, for each question, you can ‘tick’ the box for that terminal by reference to information contained on the related Terminal Characteristics Forms.

Conducting an Evaluation

An evaluation consists of inspecting each terminal in turn, and its surrounding environment, and answering the questions listed on the Merchant Evaluation Form.

In doing so, we again stress the importance of being able to **identify very small changes** compared with the information recorded on the relevant Terminal Characteristics Form. A typical evaluation might proceed as follows.

Closely inspect each terminal and answer the following questions:

- Does the terminal manufacturer’s name and model number agree with the details on the Terminal Characteristics Form?
- Does the terminal’s serial number agree with the details on the Terminal Characteristics Form (and the serial number that can be displayed on the terminal, where possible)?
- Is the terminal in its normal location? Has it moved?
- Does the terminal’s general appearance agree with the details on the Terminal Characteristics Form? Any additional small marks, cuts, or scratches around the seam, may indicate a compromise.
- Are the terminal’s security seals and labels intact, and do the written details agree with the details on the Terminal Characteristics Form? The manufacturer will have applied these labels. Do the labels appear to have been removed or tampered with? Pay close attention to color, type of paper used, design etc.
- Where applicable, do any UV-visible markings agree with that stated on Terminal Characteristics Form?

- Are the physical connections to the terminal as described on the Terminal Characteristics Form? It is not unusual for criminals to change the cable connecting the PED to an Electronic Cash Register to hide cabling for their skimmer.
- Do the number of connections, their style, type, and color of cables, match with the description on the Terminal Characteristics Form? It is not unusual for criminals to add another connector. Pictures can help to quickly identify what should be there and what (if anything) is new?
- Closely inspect the terminal for any signs that a skimming device may have been inserted. Any wires that seem out of place, or an ill-fitting shroud could indicate a compromise.
- Inspect the area around the sales desk. Are the number and type of any display stands, merchandising, and charity boxes as described on the Terminal Characteristics Form? Criminals have been known to hide a miniature camera in a charity box.
- Inspect the ceiling area above the terminals. Are there any signs of disturbance or marks that do not agree with that stated on the Terminal Characteristics Form? Check that no ceiling tiles have been lifted or moved. Look for any small holes in the ceiling that may indicate the presence of a camera.
- Check the total number of terminals in use. Has a 'new' terminal appeared?
- Check the number and location of the security cameras. Any additional cameras should be investigated, however 'official' they may look.
- Inspect the general area around the terminal. Has anything changed that could indicate a compromise? Has any new electronic equipment appeared around the cash desk?

WARNING!

Should the checklist identify that an attack has taken place, or identify a hidden camera or skimming device, do not touch or move anything. Instead, immediately contact your local law enforcement and your acquirer or service provider.

Secure the area with an 'out of order sign' and do not allow any transactions to be performed on suspicious equipment.

Appendix A Risk Assessment Questionnaire

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

Risk Assessment.....	A-1
----------------------	-----

Risk Assessment

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’.

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

Risk Assessment Questionnaire

Risk Assessment

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

No.	Question	Finding	Value	Your Score
27.	Are all your terminals PCI POS PED approved?	Yes No Don't know	0 1 1	
28.	Are your wireless-enabled terminals MasterCard PTS approved?	Yes No Don't know	0 1 1	
29.	Have your premises already been the subject of a credit card fraud attack?	Yes No Don't know	0 1 1	
30.	Have your premises been burgled within the last six months?	Yes No	1 0	
TOTAL SCORE:				

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.....	B-1
Merchant Evaluation Checklist.....	B-2

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 Location:	Location when not in use:
Make of Terminal:	Model Number:
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?	
Connection #1: Connector type, color of lead	
Connection #2: Connector type, color of lead	
Connection #3: Connector type, color of lead	
Connection #4: Connector type, color of lead	
How many connections in total (all leads, plugs, aeriels, 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?					
Is the manufacturer's name correct?					
Is the model number correct?					
Is the serial number printed on the label correct?					
Is the serial number displayed on screen correct?					
Is the color and general condition of the terminal as described, with no additional marks or scratches (especially around the seams)?					
Are the manufacturer's security seals and labels present, with no signs of peeling or tampering?					
Are the manufacturer's security markings and reference numbers as described?					
Are any expected Ultra-Violet markings present, and as described?					
Are all connections to the terminal as described, using the same type and color of cables, and with no loose wires or broken connectors?					
Count the number of connections to the terminal. Does this agree with the number stated?					
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?					
Is the condition of the ceiling above the terminal the same as described, with no additional marks, fingerprints, or holes?					
Is the total number of terminals in use the same as the number of terminals officially installed?					
Where surveillance cameras are used, is the total number of cameras in use the same as the number of cameras officially installed?					