

**PIN Pad Management Best Practices v1.2.doc**



**© Copyright, 2006, VeriFone  
The following text is protected by law from any form  
of duplication unless prior permission is obtained from  
the officers of the aforementioned company**

Filename: PIN Pad Management Best Practices v1.2.doc

# 1 Document History

Version	Author	Date	Description
0.1	Chris Madden	June 7, 2006	Initial Version.
0.2	Chris Madden	June 12, 2006	Updated for release.
0.3	Chris Madden	June 15, 2006	Added details for each best practice.
0.4	Chris Madden	June 16, 2006	Updated for release.
1.0	Chris Madden	June 16, 2006	Release.
1.0.1	Chris Madden	June 17, 2006	Minor edits.
1.1	Chris Madden	Nov 20, 2006	Rebranded to VeriFone. Minor amendments.
1.2	Chris Madden	Nov 28, 2006	Updated following meeting with Dave Faoro and Sean Gallagher.

# 2 Table of Contents

1 Document History.....	2
2 Table of Contents.....	2
3 References.....	3
4 Introduction.....	3
PIN Pad Management Best Practices .....	4
4.1 Administrative.....	5
4.1.1 Track serial numbers on all sites down to each POS/ECR.....	5
4.1.2 Secure any PIN Pads in transit.....	5
4.1.3 Ensure PIN Pads and POS systems are running the latest software updates.....	5
4.1.4 Check the accreditations / references of any consultants and third parties including technicians. Require they show ID and sign a service log.....	5
4.1.5 Improve staff vetting, check references of all new staff including full name, address, telephone number and social security number.....	5
4.1.6 Produce a security policy, detailing the secure operation and configuration of the PIN Pad and terminal.....	5
4.1.7 Make staff aware of security, and aware of their role in maintaining that security.....	5
4.1.8 Enforce Separation of Duties and Least Privilege and Rotation.....	5
4.1.9 Become familiar with proper card processing procedures.....	6
4.1.10 Become familiar with card security features.....	6
4.1.11 Periodically perform an independent site audit.....	6
4.1.12 Periodically audit service log.....	6
4.1.13 Use and retain accurate shift schedules so that a staff audit trail is available.....	6
4.1.14 Retain and backup master receipts and log files securely.....	6
4.1.15 Examine suspect devices.....	6
4.1.16 Check that the serial number reported by the PIN Pad matches the serial number on the label.....	6
4.1.17 Report stolen or malfunctioning devices immediately to PIN Pad vendor.....	6
4.2 Physical.....	7
4.2.1 Secure the PIN Pads on the counter (while still meeting disability requirements).....	7
4.2.2 Place cable clips/locks with tamper-evident labels on the PIN Pad cable.....	7
4.2.3 Become familiar with the POS equipment so that any foreign devices such as pin-hole cameras or extra cables are recognized.....	7
4.2.4 Place tamper-evident labels on PIN Pad strategic locations.....	7
4.2.5 Check tamper-evident labels for evidence of interference.....	7
4.2.6 Use CCTV and store CCTV footage offsite, inaccessible to store staff.....	7
4.3 Technical.....	7
4.3.1 Ensure that POS systems check for a valid PIN Pad serial number periodically.....	7

### **3 References**

1. POS/POI Terminal Security Best practices to application developers, system integrators, and end users, Mastercard, February 2006 Draft V02
2. Visa Fraud Prevention for merchants  
<http://merchants.visa.com/prevention/main.jsp>
3. Payment Card Industry (PCI) Data Security Standard  
<https://www.pcisecuritystandards.org>

### **4 Introduction**

This document analyses the Best Practices for PIN Pad Management from a sound security perspective to minimize fraud.

The intended audience is merchants and system integrators who use POS products.

The “Prevention is better than cure” approach is taken to prevent, detect and then correct fraud with most emphasis being placed on prevention.

To encourage reading of these best practices they have been condensed and categorised into one page.

## PIN Pad Management Best Practices

	Prevent	Detect	Correct
Administrative	Track serial numbers on all sites down to each POS/ECR		
	Secure any PIN Pads in transit		
	Ensure PIN Pads and POS systems are running the latest software updates		
	Check the accreditations / references of any consultants and third parties including technicians. Require they show ID and sign a service log		
	Improve staff vetting, check references of all new staff including full name, address, telephone number and social security number		
	Produce a security policy, detailing the secure operation and configuration of the PIN Pad		
	Make staff aware of security, and aware of their role in maintaining that security		
	Enforce Separation of Duties and Least Privilege and Rotation		
	Become familiar with proper card processing procedures		
	Become familiar with card security features		
		Periodically perform an independent site audit	
		Periodically audit service log	
		Use and retain accurate shift schedules so that a staff audit trail is available	
		Retain and backup master receipts and log files securely	
	Examine suspect devices		
	Check that the serial number reported by the PIN Pad matches the serial number on the label.		
		Report stolen or malfunctioning devices immediately to PIN Pad vendor	
Physical	Secure the PIN Pads on the counter (while still meeting disability requirements)		
	Place cable clips/locks with tamper-evident labels on the PIN Pad cable		
	Become familiar with the POS equipment so that any foreign devices such as pin-hole cameras or extra cables are recognized		
	Place tamper-evident labels on PIN Pad strategic locations.	Check tamper-evident labels for evidence of interference	
		Use CCTV and store CCTV footage offsite, inaccessible to store staff	
Technical	Ensure that POS systems check for a valid PIN Pad serial number periodically	Ensure that POS systems check for a valid PIN Pad serial number periodically	

## **4.1 Administrative**

### **4.1.1 Track serial numbers on all sites down to each POS/ECR**

A list should be maintained of PIN Pads deployed on site.

The configuration of what PIN Pads are connected to what POS should also be recorded.

This configuration should only be changed by qualified service technicians. Any configuration changes should be approved and recorded.

Periodically, check PIN Pad serial numbers against the list to ensure they are valid PIN Pads.

### **4.1.2 Secure any PIN Pads in transit**

PIN Pads should be secured in transit to ensure they arrive without interference at their destination. A log of serial numbers for PIN Pads in transit should be kept separately so that if PIN Pads are stolen or lost in transit they can be blacklisted.

### **4.1.3 Ensure PIN Pads and POS systems are running the latest software updates**

Check with the PIN Pad and POS vendors to ensure software is up to date to include the latest security features and bug fixes.

### **4.1.4 Check the accreditations / references of any consultants and third parties including technicians. Require they show ID and sign a service log**

Social engineering is sometimes employed to commit fraud; a fraudster acts as a service technician or consultant to allow them to gain unauthorized access.

All technicians, consultants and third parties should be required to show their ID and sign a service log. The details of the visit should be communicated in advance to the merchant by someone the merchant knows.

### **4.1.5 Improve staff vetting, check references of all new staff including full name, address, telephone number and social security number**

Members of staff may collude with a fraudster or commit fraud themselves. This may be due to coercion. It is important that all staff is vetted thoroughly using references where possible. Full contact details verified against ID or utility bill should be obtained.

### **4.1.6 Produce a security policy, detailing the secure operation and configuration of the PIN Pad and terminal**

It should be clear who can perform what operations on a PIN Pad and terminal and how these are configured. This should be captured from the highest level in a security policy, to the lowest level in a procedure manual. The procedure manual should cover:

- maintenance and service
- security
- operation

It should be available in-store at all times and contain all relevant contact details for external parties.

### **4.1.7 Make staff aware of security, and aware of their role in maintaining that security**

- Incorporate fraud prevention into staff training sessions
- Post fraud prevention reminders and materials near registers and in staff areas
- Offer rewards or incentives for staff who prevent a fraudulent transaction

### **4.1.8 Enforce Separation of Duties and Least Privilege and Rotation**

#### **Separation of Duties**

Ensure that staff duties are separated such that one staff member does not have the ability to abuse their position to commit or conceal fraud e.g. a separate member of staff other than the cashier should be responsible for checking transaction totals.

#### **Least Privilege**

Staff should have only the minimum required access rights to perform their duty but no more e.g. cashier should not have access to the terminal or PIN Pad service menu.

## **Rotation**

Staff should be rotated regularly to help prevent and detect fraud. E.g. cashiers could be allocated to different tills each time. Each cashier could perform quick checks on PIN Pad when starting their shift.

### **4.1.9 Become familiar with proper card processing procedures**

Refer to:

- “POS/POI Terminal Security Best practices to application developers, system integrators, and end users”, Mastercard, February 2006 Draft V02
- “Merchant Services Manual”, Visa, 15861 (03/04)
- “Merchant Services Manual”, Mastercard, MC014USD (03/04)

### **4.1.10 Become familiar with card security features**

Refer to:

- “Merchant Services Manual”, Visa, 15861 (03/04)
- “Merchant Services Manual”, Mastercard, MC014USD (03/04)

### **4.1.11 Periodically perform an independent site audit**

A random site audit performed periodically by an external party will aid in ensuring best practices are employed. It may also detect any inappropriate configuration or behaviour.

### **4.1.12 Periodically audit service log**

The service log that records the who/what/where/when/why of a technician visit should be periodically audited by central to ensure that all servicing was approved.

### **4.1.13 Use and retain accurate shift schedules so that a staff audit trail is available**

Schedules of “what staff worked when” should be maintained to help with any investigations or enquiries that may arise at a future date.

This will also act as a deterrent to staff to commit fraud as they are accountable for their actions.

### **4.1.14 Retain and backup master receipts and log files securely**

Master receipts and log files should be retained and backed up off site. They should not contain any sensitive data.

### **4.1.15 Examine suspect devices**

To non-invasively determine if skimming circuitry has been added, a device can be weighed. Additionally, the merchant card door (if any) can be unscrewed.

Skimming circuitry adds additional weight to a PIN Pad. If a device weighs more than usual, it should be reported as a suspect device.

The merchant card door can be opened to visually inspect if any additional circuitry has been added.

### **4.1.16 Check that the serial number reported by the PIN Pad matches the serial number on the label.**

These should match. The serial number can usually be returned from the PIN Pad via the API. The serial number is usually on a label on the base of the PIN Pad.

### **4.1.17 Report stolen or malfunctioning devices immediately to PIN Pad vendor**

Any PIN Pad or terminal that is stolen, malfunctions, or appears to have been interfered with should immediately be reported to internal security personnel and to PIN Pad vendor. This will ensure the device is replaced with a known-good device as soon as possible and minimize fraud.

## 4.2 Physical

### 4.2.1 Secure the PIN Pads on the counter (while still meeting disability requirements)

In some cases, PIN Pads are forcefully removed from a counter top. To prevent this, the PIN Pad should be secured to the counter top e.g. using a steel mount. However, it is important that disability requirements are also met.

### 4.2.2 Place cable clips/locks with tamper-evident labels on the PIN Pad cable

Cable clips make it more difficult to forcefully remove a device from a store but are relatively easy and inexpensive to deploy.

Tamper-evident labels can be added to these cable clips/locks to detect attempted removal or re-insertion of a PIN Pad.

### 4.2.3 Become familiar with the POS equipment so that any foreign devices such as pin-hole cameras or extra cables are recognized

System integrators, technicians and store staff should be familiar with PIN Pad and terminal equipment to be able to recognize any foreign devices that have been inserted to commit fraud.

### 4.2.4 Place tamper-evident labels on PIN Pad strategic locations.

The PIN Pad vendor can advise on sourcing and positioning tamper-evident labels.

### 4.2.5 Check tamper-evident labels for evidence of interference

Tamper-evident labels that cover the housing screws should be checked periodically by staff to ensure they are intact. If the label is damaged then it should be reported immediately.

### 4.2.6 Use CCTV and store CCTV footage offsite, inaccessible to store staff

Closed Circuit Television cameras should be used and footage retained to aid in subsequent investigations. This should not be accessible to staff.

## 4.3 Technical

### 4.3.1 Ensure that POS systems check for a valid PIN Pad serial number periodically

The system integrator should ensure that the POS/ECR periodically checks for a valid PIN Pad serial number. This will detect if any PIN Pad has been removed or a foreign PIN Pad inserted. The POS should blacklist any removed or foreign PIN Pads.

The host system should periodically monitor the PIN Pads to detect if any PIN Pad has been removed or a foreign PIN Pad inserted. The POS should blacklist any removed or foreign PIN Pads.

The higher the rate of this polling, the more effective it is.