

INDUSTRY NEWS FLASH

February 26, 2007



Recently there have been news stories about PIN Pad tampering and compromised consumer account information. VeriFone wants to assure you that none of its VISA PED or PCI PED (Payment Card Industry PIN Entry Device) approved terminals were part of the recent tampering stories and that solutions such as the VeriFone MX800 Series meet all current PCI PED Security Requirements, including tamper prevention and detection. It is our understanding that the recently publicized tampering events were targeted at pin entry devices that were purchased and installed prior to formal industry data security requirements were in place.

In this *Industry News Flash* we want to explain the process of tampering, review the current industry security requirements designed to prevent tampering, provide you with vital information about the security of your current payment terminal and advise you on steps to take to improve PIN Pad Security.

Tampering, generally involves insertion of a 'bug' into a PIN Pad to capture credit or debit card account numbers, magnetic stripe data, and consumer PINs. This is similar to other stories you may have heard about criminals inserting 'bugs' into ATMs or Gas Pumps. A commonly used tactic has been for a criminal to purchase a similar model of PIN Pad device used by a targeted merchant on the resale market, and a 'bug' is inserted into that device. This tampered device is then somehow installed in place of the merchants existing PIN Pad device where it can begin to fraudulently gather consumer information. There are several mechanisms for the criminal to collect this information, such as, simply retrieving the tampered device with its memory contents at a later date, or in some cases the information may be transmitted in real time over a wireless connection to another computer, or even transmitted through the merchant's own computer network to a remote computer. Currently, law enforcement agencies have not released any of the tampering details in these recent cases, so we do not know what method was used to get the tampered units installed or to retrieve the compromised data.

The industry is keenly aware of this potential liability, and both VISA PED and PCI PED Security standards specify a series of requirements PIN Pad manufacturers must meet in order to dramatically reduce the risk of tampering. These requirements include the following (Preceded with the requirement number.):

A2.2: The implementation of the PED is such that penetrating and then altering the PED so as to disclose future PINs (e.g., inserting a PIN disclosing "bug" or making PIN-disclosing functional modifications) so damages the PED that either (1) it becomes inoperative or (2) the damage is so severe that it has a high probability of detection before the PED is placed (back) into operational use.

A3: It is not feasible to penetrate the PED or ICC reader A to make any additions, substitutions, or modifications to either the PED or ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring specialized skills and equipment not readily available and:

- *Requiring that the PED or ICC reader be removed from its normal location for at least ten (10) hours, so that there is a high probability that the absence and/or re-appearance of the PED or ICC reader will be noted and reported before it is placed back into operational use or*
- *So damages the PED or ICC reader that either (1) it becomes inoperative or (2) the damage is so severe that it has a high probability of detection by the merchant and/or the cardholder before the PED or ICC reader is placed (back) into operational use.*

A4: If the PED or ICC reader A permits access to internal areas (e.g., for service or maintenance), then it is not possible using this access area to insert a pin disclosing bug. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper resistant/responsive enclosures), or it has a mechanism so that access to internal areas causes the immediate erasure of sensitive data.

A5: The security of the PED is not compromised by altering:

- *Environmental conditions.*
- *Operational conditions*

(An example includes subjecting the PED to temperatures or operating voltages outside the stated operating ranges)

A6: Sensitive functions or information are only used in the protected area(s) of the PED. Sensitive information and functions dealing with sensitive information are protected from modification without the expenditure of at least US \$25,000 per PED.

A7.3: For active display devices, cryptographically based controls are utilized to control the PED display and PED usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the PED. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.

A9: There is no feasible way to determine any entered PIN digit by monitoring sound, electromagnetic emissions, power consumption or any other external characteristic available for monitoring, even with the cooperation of the terminal operator or sales clerk without the expenditure of at least US \$25,000 per PED to defeat or circumvent.

A11: The design of the PED or ICC reader is such that it is not practical to construct a duplicate PED or ICC reader from commercially available components. For example, the casing used to house the device's electronic components is not commonly available.

B1: The PED performs a self-test upon start up and at least once per day to check firmware, security mechanisms for signs of tampering, and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.

B4: If the PED implements remote firmware updates, the device cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected or all secret cryptographic keys are erased.

In summary these requirements are designed to prevent tampering, render the device inoperable in the event of tampering, and prevent unauthorized software applications from running on the PIN Pad or terminal.

To provide you with the most up-to-date and complete information, we have also enclosed a copy of the PCI POS PIN Entry Device Security Requirements Manual, Version 1.3a, dated November 2006. Additional information may also be found on the VISA web site at:

<http://partnernetwork.visa.com/dv/pin/main.jsp>.

From a security standpoint, there are three categories of PIN Entry devices.

Non-Approved Devices

Prior to 2004, there were only minimal standards governing the manufacture of PIN Entry devices. Primarily, the protection of the master keys, key encryption schemes and proper software operation of the device were the only things required. Validation of software requirements and tamper prevention and detection were left to the individual manufacturer. These devices are typically referred to as “non-approved” devices. This is precisely the category of device that was compromised by tampering in the incident announced this weekend. Current card association regulations require that these devices be removed from service by July 10, 2010. However, due to the risk of a tampering compromise, retailers may wish to consider replacing these devices sooner.

Visa PED Approved Devices

The second category of PIN Pad or terminal device is the VISA PED approved device. All units sold after January 1, 2004 had to conform to VISA PED requirements. However, this category of devices can not be sold after December 31, 2007. At this point in time any device manufactured to conform to VISA PED requirements does not have a sunset date. That is, there is no requirement that retailers remove them from service.

PCI PED Approved Devices

The final category of PIN Pad or terminal devices is the PCI PED devices. These units have been on the market for about two years, and only products meeting PCI PED requirements may be purchased after December 31, 2007. These devices are the most secure and comply with current security standards. VeriFone’s MX800 Series solutions all meet PCI PED security requirements today.

How protected are your customers data today? Here is important information about VeriFone’s products:

PIN Pad 100 – Non Approved
PIN Pad 102 – Non Approved
PIN Pad 1000 – Non Approved
PIN Pad 2000 – Non Approved
Everest – Non Approved
OMNI 490 – Non Approved
Nurit 202 – Non Approved
Nurit 252 – Non Approved
Nurit 272 – Non Approved
Nurit 2085 – Non Approved
Nurit 3000 – Non Approved

SC5000 – VISA PED Approved
Everest Plus – VISA PED Approved
OMNI 3740 – VISA PED Approved
OMNI 3750 – VISA PED Approved
OMNI 7000 – VISA PED Approved
OMNI 7100 – VISA PED Approved
Nurit 222 – VISA PED Approved
Nurit 292 – VISA PED Approved
Nurit 8100 – VISA PED Approved
Nurit 8320 – VISA PED Approved

PIN Pad 1000SE – VISA PED Approved with PCI PED Approval Pending
Vx 510 – VISA PED Approved with PCI PED Approval Pending

Vx 610 – VISA PED Approved with PCI PED Approval Pending

SC5000 M5 – PCI PED Approved
MX830 – PCI PED Approved
MX 850 – PCI PED Approved
MX870 – PCI PED Approved
Vx 570 – PCI PED Approved
Vx 670 – PCI PED Approved
Qx 720 – PCI PED Approved
Nurit 293/2930 – PCI PED Approved
Nurit 8000 – PCI PED Approved
Nurit 8210 – PCI PED Approved
Nurit 8400 – PCI PED Approval Pending

If you are currently using a competitive terminal, you can visit the VISA web site to determine what level of security your product currently conforms to. If the product is not listed at all, it is an “unapproved product.” If the product is listed with a renewal date of December 31, 2007, then it is a VISA PED approved product. If the renewal date is December 31, 2014, then the product is PCI PED approved product.

What should you do to improve the security of your PIN Pads? Here are some suggested first steps, regardless of what level of compliance your product has.

1. Immediately perform a visual inspection on every terminal. If the inspector notices anything that looks out of the ordinary, have the unit checked by an authorized repair facility.
2. Have the inspector verify that the serial number printed on the bottom of the terminal matches the internally stored serial number. Immediately remove from service any devices where these serial numbers do not match.
3. Implement a procedure to require all repair technicians who visit your stores log in, verify their identity, and do not allow them to work on PIN Pads unaccompanied.
4. Review the installation of your PIN Pads. They should be mounted on the counter, unplugging cables should require more than turning the unit over, and you may want to consider locking stands. If you are interested, VeriFone is developing locking stands. Contact your VeriFone Account Executive for more details.
5. Review your POS to PIN Pad terminal interface to determine if it tracks or identifies the serial number of the attached PIN pad. If not, consider implementing such a software security scheme.
6. Only purchase PIN pads from a manufacturer or manufacturer’s authorized partner. Unauthorized resellers, such as may be found online at sites such as EBAY, may potentially sell devices that are already compromised, whether intentional or unwittingly.
7. For similar reasons, have your PIN Pads repaired at the manufacturer or an authorized manufacturer’s repair center which has completed a TG3 Key Injection audit.

VeriFone is in the process of assembling an Industry Best Practices Guide to PIN Pad deployment, monitoring and security which will be released later this week. When it is available, we will send it to you. In the meantime, if you have any security related questions, please contact your VeriFone Account Executive.

Sincerely,

Dave Faoro
VP Product Security and Systems Architecture