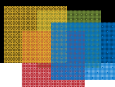




## PCI PED Deadline Looms

*Older, non-secure PIN pads and terminals are a tempting target for criminals hoping to gain access to cardholder data. The deadline for removing these devices from service is looming. With card fraud always on the move and security standards evolving quickly, it's hard to keep up. But ISOs, ISVs and resellers need to work with merchants to complete the upgrade process before July 2010.*



## Executive Summary

Criminals are increasingly targeting older, non-secure PIN pads and terminals as a relatively easy means to gain access to cardholder data. The liability from these attacks is increasingly being placed squarely at the feet of merchants and acquirers.

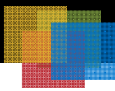
The industry, through the PCI Security Standard Council and individual card brands, has agreed on more stringent security requirements embodied in the PCI PED standard.

Manufacturers may now supply only PCI PED approved devices for PIN entry use. In-use devices that predate the Visa PED standard--known as "never approved" devices--are required to be removed from service by July 2010.

The compliance clock is ticking. ISOs, ISVs and resellers have an opportunity to work with merchants in reviewing security requirements and upgrading to compliant PIN pads. It is estimated that more than 500,000 devices that predate security certifications are in use in the U.S. market currently.

'We saw an explosion of attacks targeting PIN data in the previous year. These PIN-based attacks hit the consumer much harder than typical signature-based counterfeit attacks.

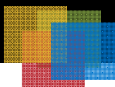
- Verizon2009 Data Breach Investigations Report



---

## Content

Executive Summary	2
Criminal Opportunities	4
The Security Mandate	5
PCI PED Implementation	6
What is PCI PED?	7
A PCI PED Upgrade Solution	8
Conclusion: Why Wait?	9



## Criminal Opportunities

The "2009 Verizon Business Data Breach Investigations Report" examined 98 confirmed data breaches, which compromised almost 300 million consumer records. Of these breaches, 81 percent of the organizations "were not Payment Card Industry (PCI) compliant," according to Verizon.

Many of these breaches had nothing to do with PIN pad compromises, but gaining PINs by compromising some element of a computer network is now the primary game in town for some criminal organizations.

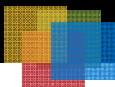
Verizon's data indicated that 75 percent of the breaches it investigated involved the retail (31 percent), financial services (30 percent) and food & beverage (14 percent) industries. And, the report stated, only one-third of the cases investigated had been publically disclosed!

Criminal breaches range from the highly sophisticated computer networking assaults, to more simplistic efforts that might be thought of as the equivalent of "smash and grab" attacks. Large transaction processors have reported placement of "malware" programs on their networks that were designed to scoop up millions of cardholder account numbers and other information. But in other cases, criminals simply replace an in-place terminal with an identical looking system that has been bugged.

Large grocery chains such as Stop & Shop and Albertsons reported in 2007 that criminals essentially breezed into unattended checkout lanes and swapped out PIN pads, returning later to reclaim the devices which by then had captured and stored hundreds of account numbers and associated PINs.

In February 2009, according to The News-Journal of Delaware, two men pleaded guilty to placing a skimmer at a Rite Aid counter that scooped up account numbers and PINs they were able to use to make counterfeit cards with which they stole more than \$500,000 from bank accounts.

For small businesses, breaches can be devastating. The Kalamazoo Gazette reported in June 2009 that two locally owned Spicy Pickle restaurants went out of business due to the impact of a hacking incident that allowed criminals to scoop up accountholder information. Restaurant co-owner Terry Henderson told the newspaper, "We never recovered our sales levels. We never came close."



## The Security Mandate

Criminal organizations have compromised older, less secure payment terminals by installing bugs to collect private credit card and debit information.

It is believed that approximately a half-million never approved devices are still in use in the U.S. market. While breaches at large retailers and processors have generated news headlines, due to the volume of compromised accounts, smaller merchants represent a much broader problem.

Visa in 2007, for example, noted that, "While less than 5 percent of potentially exposed accounts are stolen from small businesses, more than 80 percent of all identified compromises since January 1, 2005 occurred at small businesses."

In these cases, the criminal organizations either insert a bug into an in-place device or they obtain the same model terminal that a retailer uses, into which they insert a bug and then substitute the tampered device for the retailer's terminals. The bugs can store card data for later retrieval or in some cases are set up to transmit the information to another computer.

The payment industry has long recognized the need to stay ahead of criminal elements by requiring ever more secure device techniques and technologies that protect PINs, to make it difficult to tamper with devices and to implement safety protections to alert merchants and acquirers to tampering.

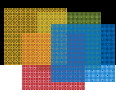
Visa in 2004 required that new installations connecting to its payment network be certified as meeting its requirements for PIN Entry Devices - this became known as the Visa PED standard.

Also in 2004, Visa and MasterCard agreed to align their separate PED requirements into an industry-wide standard, which became known as the Payment Card Industry PIN Entry Device, or PCI PED, standard. Subsequently, Visa, MasterCard, JCB, American Express Co. and Discover Financial Services LLC collaborated on the PCI Data Security Standard, a broader initiative covering the storage, transmission and processing of cardholder data.

In 2006, the PCI Security Standards Council was formed by the major card brands to oversee security standards and in April 2007, Visa, MasterCard and JCB formally transferred responsibility for PCI PED to the council, providing a more formal structure for future development of PED requirements.

In 2005, Visa announced a global mandate for Triple Data Encryption Standard (TDES) usage and established July 1, 2010, as the date for global compliance. This mandate requires that all cardholder PINs be TDES protected from the point of transaction to the issuer.

■ Visa USA



## PCI PED Implementation

The evolution of PED standards has been a source of confusion to merchants, but to simplify these changes and their impact it is helpful to regard PED devices in three classes:

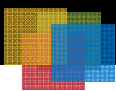
- “Never approved” devices which have never been certified to the Visa PED or later standards and must be removed from service after July 1, 2010
- Pre-PCI - those devices that were certified to the Visa PED standard, which among others things requires the devices be capable of using Triple DES (often referred to as TDES or 3DES) encryption. As of December 31, 2007, these systems can no longer be newly deployed
- PCI PED - those which meet the newer requirements and the only systems approved for deployment as of January 1, 2008

Prior to 2004, the manufacture of PIN Entry devices was governed by only minimal standards. 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.

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. The final category of PIN pad or terminal devices is the PCI PED devices, which are the most secure and comply with current security standards. Only those products meeting PCI PED requirements may be purchased after December 31, 2007.

Many manufacturers have upgraded Visa PED device types with PCI PED functions. As such, there is no easy way to tell whether you are looking at a Visa PED or PCI PED approved system. In most cases, the device just has a new part number. Contact your acquirer or device manufacturer or reseller to find out which ones are compliant.

The PCI Security Standards Council now has responsibility for creating and implementing security standards, including PCI PED, while each card brand is responsible for how it will enforce those standards and how it will penalize merchants and acquirers who violate requirements.



## What is PCI PED?

PCI PED is a targeted program specifically intended to enforce hardware security of devices that accept consumer PINs and house secret encryption keys of the acquirer, including how the PED is produced, controlled, transported, stored and used throughout its life cycle.

According to the PCI Security Standards Council, "PCI PED Security Requirements are primarily concerned with device characteristics impacting the security of the PIN Entry Device used by the cardholder during a financial transaction."

The PCI PED requirements encompass physical security, logical security and "device management up to the point of initial key loading..."

Furthermore, "The physical security characteristics of the device are those attributes that deter a physical attack on the device—for example, the penetration of the device to determine its key(s) or to plant a PIN-disclosing "bug" within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a clear-text PIN-encryption key."

Device management pertains to, "how the PED is produced, controlled, transported, stored, and used throughout its lifecycle."

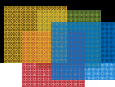
The PCI PED standard will be updated every three years to accommodate changing security realities.

The card brands mandated that, as of December 31, 2007, acquirers and merchants only deploy PCI PED approved devices. Furthermore, they set July 1, 2010, as the date by which unapproved devices must be removed from service. No such replacement date has been set for Pre-PCI devices, although they cannot be installed except as replacement for existing in-place PIN pads.

Visa has chosen to implement the following regulations in order to transition to PCI PED compliance:

October 1, 2009—Acquirers must submit to Visa a summary TDES compliance status report and plan to achieve full compliance for sponsored attended POS activity.

August 1, 2012—Acquirers may be assessed fines for sponsoring any non-TDES compliant merchants or agents.



## A PCI PED Upgrade Solution

For merchants, the compliance window is sliding shut quickly. Although Visa has indicated it won't impose penalties until 2012, acquirers have the ability to penalize merchants once the July 1, 2010 cutover arrives.

Recognizing the challenges faced by acquirers and merchants in achieving full PCI PED compliance, VeriFone enhanced the PINpad 1000SE to provide an easy upgrade solution.

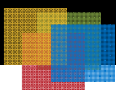
The PCI PED approved PINpad 1000SE is ergonomically designed for ease of use and handling, plus it provides the added versatility of USB or serial connectivity.

Fully backwards compatible with the previous PINpad 1000SE and the NURIT 222, it's a simple upgrade solution for merchants with those devices who need to meet the new PCI PED security standard. Additionally, it is now available with contactless, combining two payment peripherals into one space-saving device.

As a drop-in replacement for a previous PIN-based device, the PINpad 1000SE minimizes application rework and eases the transition to the newest PIN security standard

The PINpad 1000SE features comprehensive security including 3DES encryption, VeriShield Security Scripts, Master/Session and DUKPT key management; and, VeriShield file authentication.

Not only is the PINpad 1000SE but when attached to a non-compliant device, the combination becomes a compliant solution.



## Conclusion: Why Wait?

Many merchants are unaware or confused over target dates for implementation of PCI PED approved devices. Many may be tempted to put off PIN pad upgrades to some future time. But there are several reasons not to delay

- In 2007, Visa mandated that acquirers submit plans for identifying security risks for smaller merchants, whom it classifies as Level 4, and to, “Apply targeted compliance measures to merchant subgroups...”
- While Visa may not level fines prior to 2012, acquirers will still be liable for any breaches with non-compliant devices after July 1, 2010—they in turn may fine ISOs who are supporting non-compliant merchants, and those ISOs may levy some or all of that cost on the merchant.
- Acquirers may implement more aggressive compliance schedules than mandated by Visa and PCI SSC.
- Acquirers bringing new merchants on board must ensure they are compliant now.

VeriFone’s design of payment systems has placed a premium on future-proofing so that acquirers, ISOs and merchants can utilize today’s solutions with assurance they will still be viable and supported in subsequent years.

For further information about PCI PED standards, call your VeriFone sales representative, or on the web go to [www.verifone.com/pciped](http://www.verifone.com/pciped).

Copyright © 2009 VeriFone. All rights reserved. No portion of this document may be reproduced or distributed in any form or by any means without the prior written permission of said company. All trademarks are the property of their respective owners