



PCI PED Security Requirements Educational Package for Merchants

August 2009

Introduction

VeriFone understands that merchants have a lot of things to worry about and that the ever changing security standards are hard to keep up with and often times difficult to understand. Because security is so complex, merchants are sometimes not in compliance simply because they don't know which standards apply to them.

We have taken the work out of security, sifted through all of the information out there and compiled what merchants need to know in a simple, easy to understand package. Our goal is to inform small to mid-sized merchants whether they are compliant and what they need to do to become compliant.

To review, there are three different mandates from Visa that must be met by US merchants by July 1, 2010. These are:

- All non-certified payment terminals on which PIN debit transactions are conducted must be removed from service. This includes any terminal that is not either VISA PED or PCI PED.
- All debit card PINs must be encrypted in TDES from the payment terminal
- All applications that "store, process, or transmit cardholder information" must be PA-DSS or PABP compliant.

What is PCI PED?

PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions. Merchants should only use PIN entry devices that are tested and approved by the PCI SSC. The PCI PED standard will be updated every three years to accommodate changing security realities. PCI PED security requirements only affect devices that are used for debit card payment acceptance.

Important Dates

- July 1, 2010 - "Never approved" devices which have never been certified to the Visa PED or later standards must be removed from service by this date. Acquirers can fine non compliant merchants and ISOs anytime after July 1, 2010
- August 1, 2012 the date by which acquirers may be assessed fines for sponsoring any non-TDES compliant merchants or agents from Visa.

Product Charts

We have included the most compatible direct replacement as well as the recommended upgrade.

Product Upgrade Chart for Multi-lane Retailers

PCI PED COMPLIANCE CHART		
MANUFACTURER	VISA PED APPROVED/NON PED APPROVED DEVICES*	COMPARABLE PCI PED APPROVED REPLACEMENT DEVICES*
VeriFone	Omni 7000	MX 830, MX 850, MX 860
	Omni 7100	MX 870, MX 880
	PP1000	PP1000sE, V ^x 810
	Everest	MX 830, MX 850, MX 860
HHP	TT8810	MX 870, MX 880
	TT3101 (same as symbol 3100)	MX 870, MX 880
	TT8870	MX 870 with Price Checker
Hypercom	L4100	MX 870, MX 880
	S9	PP1000sE, V ^x 810
Ingenico	IVI C2000 Protege	MX 830, MX 850, MX 860
	IVI Checkmate 2100	MX 830, MX 850, MX 860
	Ingenico eN-Touch 1000 IVI Checkmate	MX 870, MX 880
NCR	5991	MX 870, MX 880
	5992 (rebranded eN-Touch 1000)	MX 870, MX 880
	4430	MX 830, MX 850, MX 860
	5945 (Ingenico 2100)	MX 830, MX 850, MX 860
Symbol	iPOS 3100	MX 870, MX 880
	PD8750 (Hypercom L4100)	MX 870, MX 880

*Check part numbers to ensure compliance.

**All trademarks mentioned herein belong to their respective owners.

Product Upgrade Chart for Countertop and Mobile Merchants

PCI PED COMPLIANCE CHART			
MANUFACTURER	VISA PED APPROVED/NON PED APPROVED DEVICES*	COMPARABLE PCI PED APPROVED REPLACEMENT DEVICES*	HIGHER FUNCTIONING PCI PED APPROVED DEVICES
VeriFone	Omni 3740	V ^x 510	V ^x 510 Ethernet
	Omni 3750	V ^x 570	V ^x 570
	NURIT 8320	V ^x 510	NURIT 8400
	NURIT 2085+	V ^x 510	V ^x 570
Exadigm	XD1000	V ^x 570	V ^x 570 (Ethernet) or V ^x 610 (CDMA)
Hypercom	T7Plus	V ^x 510	V ^x 570
	Artema	V ^x 510 GPRS	V ^x 610 or V ^x 670
	S9	PP1000sE	PP1000sE
Ingenico	Elite 712	V ^x 510	V ^x 510 or V ^x 570
	Elite 710	V ^x 510LE	V ^x 510 or V ^x 570
Way Systems	MTT1556	V ^x 670	V ^x 670

For most, adding a PP1000sE will make the solution compliant.
 *Check part numbers to ensure compliance.

Frequently Asked Questions

How do I know if I'm compliant?

check the PCI website for a list of all never-approved devices???. We've listed the most compatible VeriFone replacement. If you do not see your current device in our chart, you can also visit the PCI website for a list of approved devices or contact your merchant acquiring representative

How do I find out if my payment device is compliant?

Refer to the charts. To find out what model of device you have, look for the brand name and device name either on the front or the bottom of the terminal. This is not an all-inclusive list. Go to the PCI website or contact your merchant acquiring representative if you do not see your device on the list in this document or on the website.

Why do I need to comply by July 1 if Visa won't fine until 2012?

2012 is when Visa will fine acquirers. Acquirers, however, can fine ISOs and merchants at any time for non-compliance. You will also be liable in the case of a data breach.

How much are the fines?

We do not know how much the fines will be. We anticipate the fines will be high and will depend on the size and length of the breach. We have created a simple to use

risk calculator on our PCI PED landing page www.verifone.com/pciped. For petroleum retailers, please visit

In addition to the fines you may incur, lawsuits as well as the cost of the breach itself can add up greatly and can put a retailer out of business. Not to mention the bad press and loss of customers who will no longer trust you with their card information.

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."

I thought breaches only happened to the large retailers, not a small retailer like me. I only run 100 transactions per month. No criminal will target me.

While the large breaches are the ones that receive much of the media attention, the majority of breaches happen in small level 4 retailers that process fewer than 1 million transactions per year. According to a security report by Verizon, 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.

The economy is tough; I cannot afford the additional cost of a new terminal.

Compared to a breach or fines, the investment toward a new payment device is minimal. Plus VeriFone's products are future-proof. You can either purchase a direct replacement or upgrade to better features, more memory, faster communications. We're here to help find the perfect fit for your business.

Is there any way that I can make a current device compliant so I don't have to buy a new one?

Yes, simply add a PCI PED approved PINpad 1000SE. It's simple; just plug it into the port of your payment device and you're good to go. Purchase your VeriFone PINPad 1000SE from your payment company supplier (merchant acquirer). It should state Triple DES encrypted on the back of it.

Where can I find out more?

There are a number of other resources you may find helpful:

VeriFone Web Resources

- PCI PED Landing Page
www.verifone.com/pciped
- VeriFone Security Page

- www.verifone.com/security
- Secure Retail Payments Webpage
<http://www.verifone.com/industry-solutions/retail/payment-trends--security/secureretailpaymentscom.aspx>

PCI Security Standards Council Web Resources

- Main Page
www.pcisecuritystandards.org
- Frequently Asked Questions
www.pcisecuritystandards.org/faq.htm
- List of PCI PED approved devices
https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html
- Self-Assessment Questionnaire
www.pcisecuritystandards.org/saq/index.shtml

Additional Resources

- Visa
<http://broadcast01p.visabroadcasts.com/doc/20090422091220/5163459b29ec9fcd6f98ceddad92d3d>