PCI 1.X EXPERIENCE AND BEYOND

WHY IS THE PCI SECURITY STANDARDS COUNCIL COMING OUT WITH NEW REQUIREMENTS?

New requirements ensure that point of interaction devices/products are being tested and validated against the highest level of security.

WHY DID THE PCI PTS VERSION 1.X DEVICE CERTIFICATION EXPIRE, CAUSING THE DEVICES TO BE PLACED IN END-OF-LIFE STATUS?

Typically, PCISSC'S are regularly enhanced on a three-year cycle, based upon analyses of changes in the threat environment. The PCI PTS version 1.X devices have been targeted for compromises that have resulted in financial losses in some cases. These older devices were tested under security standards that have become outdated.

WHAT IS THE IMPACT TO THE ACQUIRER AND THEIR AGENTS FOR DEVICES PURCHASED AFTER APRIL 30, 2014?

Entities that purchase devices past the expiration date will assume liability, and there will be no liability protection from compromises, security breaches and theft of payment card data associated with the deployment of the impacted devices, unless the device is used for like-for-like repair or replacement.

ARE THERE OTHER RETIREMENT DATES THAT I NEED TO BE AWARE OF?

Yes. Here are summaries of Visa Inc. and Visa Europe's PCI PED retirement dates:

Visa Inc. PCI PED retirement dates:

Lab Evaluation Status	PED Device Type	PCI PTS Device Expiration Date	Visa Purchase Requirements	Visa Deployment Requirement	Visa Usage Requirement	Visa Sunset Mandates
PCI PED or EPP PED V1.X	Attended POS PED	April 30, 2014	Not allowed after device expiration date	Allowed if purchased prior to expiration date		Recommend device replacement
	EPP used in Unattended POS/ ATM/Kiosk					
PCI PED or EPP PED V2.X	Attended POS PED	April 30, 2017	Not allowed after device expiration date	Allowed if purchased prior to expiration date		Recommend device replacement
	EPP used in Unattended POS/ ATM/Kiosk					

Visa Europe PCI PED retirement dates:

Device Type	Approval Expiration Date	No New Deployments After ...	Retire from Use by...
PCI PED 1.X Attended/Semi-attended	April 2014	April 2014	December 2017
PCI PED 1.X Unattended	April 2014	April 2014	December 2020
PCI PED 2.X Attended/Semi-attended	April 2017	April 2017	December 2020
PCI PED 2.X Unattended	April 2017	April 2017	TBD Dependent on threat environment

Verifone®

PCI 1.X EXPERIENCE AND BEYOND

WHAT IS THE IMPACT TO AN ACQUIRER IF THEY OR THEIR AGENT DEPLOYS ENCRYPTING PIN PADS (EPPS) OR POINT-OF-SALE (POS) PIN ENTRY DEVICES (PEDS) THAT HAVE NOT BEEN EVALUATED BY A PCI RECOGNIZED LABORATORY AND ARE NOT ON THE CURRENT PCI APPROVED LIST?

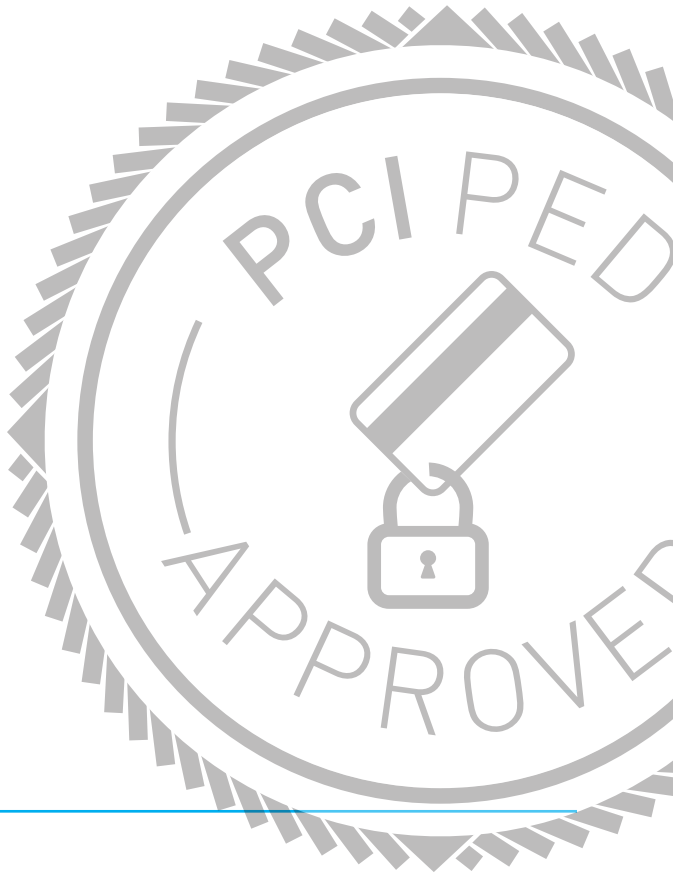
Entities deploying EPPs or POS PEDs that have not been evaluated by a PCI Security Council-recognized lab and/or are not approved by PCI at the time of purchase may be liable in the event of a compromise that is attributable to the lack of using an approved EPP or POS PED.

HOW CAN ACQUIRERS AND THEIR AGENTS ENSURE THAT THE EPPS OR POS PEDS THEY PURCHASE ARE COMPLIANT TO THE APPLICABLE PIN ENTRY DEVICE SECURITY REQUIREMENTS?

Acquirers and their agents should always look to the web site at www.pcisecuritystandards.org/pin and validate the device is listed on the web site: Model Name, Hardware Number, Firmware Number and if applicable, Application Number.

CAN I REPLACE OR REPAIR AN EXPIRED 1.X DEVICE THAT IS ALREADY IN THE FIELD?

Like-for-like repair or replacements are permitted, if the replacement is performed by the device's original purchaser or their agent, even though the approval has lapsed.
[Source: Visa General FAQ – May 2010]



Verifone®

PCI 1.X EXPERIENCE AND BEYOND

WHAT HAPPENS TO THE DEVICES THAT HAVE BEEN COMPROMISED?

The devices that have been reported as compromised have been delisted by the PCI Security Standards Council (SSC). Therefore, they are no longer PCI-PTS-approved devices.

Devices that have been compromised, as noted on www.visa.com/cisp, should be replaced with newer, more secure versions of the product, or with different models, whenever an opportunity presents itself.

WHAT DOES THE LIABILITY SHIFT REGARDING U.S. CHIP REQUIREMENTS MEAN?

Visa USA: Acquirers and merchants who do not support dynamic data (chip) by October 2015*, may be liable for counterfeit fraud. *2017 for Automated Fuel Dispensers (AFD) [Source: Visa – "Americas Merchant PIN Security Compromise Trends and Best Practices Webinar" –February 13, 2013]

- MasterCard USA: "Beginning in October 2016, a liability shift hierarchy will be introduced for ATM transactions in the U.S., as part of an effort to globally align the use of EMV technology to prevent and manage fraud in the payments ecosystem. The liability shift will apply to all MasterCard-branded products across all transactions initiated at U.S. ATMs."

[Source: MasterCard Press Release – "MasterCard Extends U.S. EMV Migration Roadmap to ATM channel", September 10, 2012] Press release web page – http://newsroom.mastercard.com/press-releases/mastercard-extends-u-s-emv-migration-roadmap-to-atm-channel/

- American Express USA: "Effective October 2015, American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. U.S. fuel merchants will have an additional two years, until October 2017, before the FLS takes effect for transactions generated from automated fuel dispensers."

[Source: American Express Press Release – "American Express Announces US EMV Roadmap to Advance Contact, Contactless and Mobile Payments", June 29, 2012] Press Release web page – http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx

WHAT ARE ADDITIONAL KEY DATES FOR THE U.S. THAT I NEED TO BE AWARE OF?

The chart below shows key dates for merchants, manufacturers and acquirers.

Event	CHIP Liability Shift – POS	CHIP Liability Shift – AFD*
Device impact	Deployed Chip devices limits liability	Deployed Chip devices limits liability
Date	October 2015	October 2017

Sources: (1) Visa – "Americas Merchant PIN Security Compromise Trends and Best Practices Webinar" – February 13, 2013
(2) MasterCard Press Release – "MasterCard Extends U.S. EMV Migration Roadmap to ATM channel", September 10, 2012
(3) American Express Press Release – "American Express Announces US EMV Roadmap to Advance Contact, Contactless and Mobile Payments", June 29, 2012

GENERAL PCI QUESTIONS

WHAT IS THE DIFFERENCE BETWEEN PCI PED AND PCI PTS?

PCI PED was changed to PCI PTS in October 2009. The new name reflects an expanding standards program that will continue to incorporate other parts of the PIN-based payment chain beyond PED and other physical devices.

WHAT IS PCI PTS (PAYMENT CARD INDUSTRY – PAYMENT TRANSACTION SECURITY)?

PCI PTS (formerly PCI PED) is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment-processing related activities. The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it.

GENERAL PCI QUESTIONS (CONT'D)

WHO IS REQUIRED TO COMPLY WITH THE PCI DATA SECURITY STANDARD (DSS)?

As defined by PCI SSC, PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Merchants in scope of PCI DSS are required to periodically (as defined by payment brands and/or their acquiring bank) validate their PCI DSS status. PCI DSS encompasses the security of point of sale devices, systems and/or networks (and their components) on which cardholder data or sensitive authentication data (or both) are stored, processed or transmitted.

Effective July 2015, PCI DSS version 3.0 added a new requirement (9.9) that addresses device management for merchants. This requirement states that all merchants must have controls in place to protect against direct physical tampering and substitution of their card-reading devices used in card-present transactions at the point of sale. That is any card swipe Point of Interaction (POI) device or terminal used in face-to face transactions (including any unattended payment terminals accepting transactions where the customer's card is present). This requirement requires a new set of additional policies, procedures, and training for merchant organizations as employees will now be responsible for inspecting and tracking/managing the inspections at all stores that have payment devices in scope of this new requirement.

WHO ENFORCES THE COMPLIANCE DEADLINE?

PCI Council does not enforce compliance of their standards; rather the payment brands are responsible.

Generally speaking compliance enforcement will be communicated through your acquiring bank.

WHERE CAN ACQUIRERS, MERCHANTS AND/OR PROCESSORS GO FOR MORE INFORMATION?

- MasterCard: Customers with general questions about device security at the POI should send an email to:
  POI Security at: poi_security@mastercard.com.

- Visa, Inc., visit:
  http://usa.visa.com/download/merchants/visa-PED-Requirements-2013.pdf

- Visa Europe:
  - For more information on the PIN Security Program me please contact Visa at: visaeuropepin@visa.com or visit www.visa.com/pinsecurity
  - Visit the Merchants page for a detailed description of Visa merchant levels of compliance criteria and validation actions:
    http://www.visaeurope.com/en/businesses__retailers/payment_security/merchants.aspx
  - Visit the Service provider page for more information on service provider compliance criteria and validation actions:
    http://www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

- American Express: For general information regarding PCI security requirements and data security, visit:
  https://www.americanexpress.com/in/content/merchant/support/data-security/merchant-information.html

Verifone®