Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL UPDATES PTS PROGRAM FOR ENCRYPTION, MOBILE

—Changes to PIN Transaction Security Program set foundation for secure point-to-point encryption and mobile payment acceptance—

WAKEFIELD, Mass., October 14**,** 2011 —The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today announced updates to its PIN Transaction Security (PTS) program that enable adoption of point-to-point encryption (P2PE) technology to support PCI DSS compliance. Version 3.1 is a result of the standard PTS development lifecycle allowing for a minor update release within 12-18 months after a major version is published, and is effective immediately, superseding version 3.0.

PTS 3.1 adds two new approval classes that facilitate the deployment of P2PE technology in payment card security efforts, building on the Secure Reading and Exchange of Data (SRED) module previously introduced in version 3.0 to support the secure encryption of account data at the point of interaction. Until now, the PIN Transaction Security program has applied to PIN acceptance devices only. With the release of version 3.1, requirements will expand for the first time to include protection of account data on devices that do not accept PIN, meaning any card acceptance device can now be PTS tested and approved and eligible to deploy point-to-point encryption technology.

Additionally, the requirements have been updated to address secure (encrypting) card readers (SCR), further facilitating the deployment of P2PE technology and the use of

—more—

open platforms, such as mobile phones, to accept payments. Merchants looking to use magnetic stripe readers (MSRs) or MSR plug-ins now can ensure these devices have been tested and approved to encrypt data on the reader before it reaches the device.

The Council published a roadmap outlining its approach to point-to-point encryption technology in the cardholder data environment late last year and recently released the PCI Point-to-Point Encryption Requirements, the first set of validation requirements in its P2PE program. Findings from its initial examination of mobile payment acceptance applications in light of the PA-DSS were published in June, and in collaboration with industry experts in an SSC-led Mobile Taskforce, the Council aims to deliver further guidance by year's end.

"We know how eager the market is to implement P2PE," said Bob Russo, general manager, PCI Security Standards Council." By releasing these updated requirements now, merchants using any type of card acceptance device will have the ability to encrypt data at the point of interaction and ensure its protection. Additionally, we've opened the standard up to address mobile devices – another area of great interest to our stakeholders."

The updated PTS Security program requirements and detailed listing of approved devices are available on the Council's website at https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php .

There will be a session devoted to PTS program updates, including a dedicated question and answer forum, at the PCI Community Meeting taking place in London, England on October 17-19. For more information or to attend the PCI Community Meetings, please visit: https://www.pcisecuritystandards.org/communitymeeting/2011/.

Additionally, the Council will host a Webinar for Participating Organizations and the public outlining the newest updates to the PIN Transaction Security program, followed by a live Q&A session.

To register for the November 8 session, please visit:

http://register.webcastgroup.com/l3/?wid=0801108115798

To register for the November 10 session, please visit:

http://register.webcastgroup.com/l3/?wid=080111011579

About the PCI Security Standards Council

The PCI Security Standards Council is an open, global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and related standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has more than 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linked-in.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###