Media Contacts

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

Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL ADDS PCI PIN SECURITY REQUIREMENTS TO PTS STANDARD

—Requirements for PIN security added after the Council takes over program management from payment card brands. —

WAKEFIELD, Mass., November 3**,** 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 that the Council is expanding the PTS standards to encompass the PCI PIN Security Requirements, formerly administered by Visa and MasterCard, to provide organizations with one set of criteria for the protection of PIN data.

After officially taking over management of the requirements earlier this year, the PCI SSC solicited feedback from the PCI community to make updates to the standard. Today's release contains a complete set of requirements for the secure management, processing and transmission of personal identification number (PIN) data at ATMs, and attended and unattended point-of-sale (POS) terminals. The PIN Security Requirements will be included in current PTS security requirements. The updated PTS program requirements and detailed listing of approved devices are available on the Council's website at https://www.pcisecuritystandards.org/security_standards/documents.php?document=PIN_Security_Requirements_v1#PIN_Security_Requirements_v1.

"Point of sale continues to be a security hotspot as criminals are using more advanced techniques to steal PIN and cardholder data," said Bob Russo, general manager of the

—more—

PCI Security Standards Council. The requirements are specifically geared toward protecting not just the devices that accept PINs but also the people and processes surrounding them."

The PCI PIN Security Requirements provide one set of criteria for protection of Primary Identification Number (PIN) data. For merchants - examples of common vulnerabilities for PIN theft that the requirements address include:

- PINs that are not protected by a secure PIN block
- Failure to use approved cryptographic devices for PIN processing
- Cryptographic keys that are non-random, not unique, and never change
- Few, if any documented PIN-protection procedures
- Audit trails or logs that are not maintained

"With this addition to the PTS requirements, we hope to strengthen POS security at merchants around the globe," noted Russo.

The Council will also host a Webinar for Participating Organizations and the public outlining the newest updates to the PIN Transaction Security program, including the PIN Security Requirements, 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=0801110115799

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

###