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 CONTINUES FOCUS ON MOBILE PAYMENT ACCEPTANCE SECURITY

- Council participates in Congressional Subcommittee Hearing on Mobile Payments -

WAKEFIELD, **Mass**., March 22**,** 2012—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 demonstrated its continued focus on mobile payment acceptance security with participation in a Congressional hearing titled "The Future of Money: How Mobile Payments Could Change Financial Services," held by the Subcommittee on Financial Institutions and Consumer Credit.

Joined by representatives from the Atlanta Federal Reserve, MasterCard, the Smart Card Alliance, and the Consumer Union, PCI Security Standards Council Chief Technology Officer Troy Leach served as an expert panelist, providing insight into security considerations when it comes to payment acceptance using mobile technology, as well as the Council's work to date and future plans in this area.

The hearing is the first in a series of three designed to examine the technology by which mobile transactions are conducted; identify potential security problems or regulatory barriers that consumers, merchants, and financial institutions might face when using mobile payment services; and consider whether statutory changes are necessary as mobile payment systems become more widely available and are increasingly used.

—more—

Participation in the hearing comes as part of the Council's and its stakeholders' focused efforts in the area of mobile acceptance security.

The area of mobile payments includes two different environments for the use of mobile devices. In the first case, merchant acceptance applications, phones, tablets and other mobile devices are used by merchants as point-of-sale terminals in place of traditional hardware terminals. The second refers to consumer facing applications where the phone is used in place of a traditional payment card by a consumer to initiate payment.

The Council's security efforts to date in this area have been concentrated on the first environment, securing the use of mobile devices as a point of sale acceptance tool.

"Mobile technology offers exciting potential to the payments space," said Troy Leach, chief technology officer, PCI Security Standards Council. "To help realize this securely, the Council is working with its global stakeholders to develop the industry standards and resources necessary for the protection of cardholder data across all payments channels, and for the reduction of fraud for consumers and businesses globally."

In 2011, the Council issued guidance on the types of payment applications that can allow organizations to accept and process payments securely using mobile technology, including a checklist resource to help explain simply and succinctly to anyone currently considering mobile acceptance solutions which types of application support PCI Standards.

The Council also identified the types of applications that fall short of security standards for secure mobile acceptance. In collaboration with industry subject matters experts, including software application developers, the Council is continuing to examine this area to determine whether the inherent risk of card data exposure in these applications can be addressed by existing PCI Standards, or whether additional guidance or requirements must be developed.

Additionally, at the end of 2011, updates to the PIN Transaction Security (PTS) Requirements addressing secure (encrypting) card readers (SCR) enabled the

deployment of point-to-point encryption technology and the use of open platforms, such as mobile phones, to accept payments.

Compliance by device vendors with these requirements now allows merchants to use plug in devices with mobile phones to swipe cards securely by first encrypting the data at the point that the card is swiped to minimize risk by making it unreadable. The mobile device acts as a conduit and has no ability to decrypt the encrypted data.

In the coming months the Council plans to release specific guidance for merchants on how to effectively use these security requirements in conjunction with encryption technology to more easily and securely accept payments using mobile technology. Later this year the Council will also produce a best practices document for securing mobile payment transactions.

PCI and mobile payment security will be a topic of discussion at the Council's Annual Community Meetings scheduled for September 12-14 in Orlando, Florida and October 22-24 in Dublin, Ireland. For more information, please visit: https://www.pcisecuritystandards.org/communitymeeting/2012/.

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 other 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 over 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.linkedin.com/company/pci-security-standards-council

Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###