Security Standards Council

Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

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

PCI SECURITY STANDARDS COUNCIL RELEASES GUIDANCE FOR MERCHANTS ON MOBILE PAYMENT ACCEPTANCE SECURITY

— Merchant education tool aimed at driving demand for secure mobile payment acceptance options —

WAKEFIELD, Mass., February 14, 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards published the *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users*. The guidance educates merchants on the factors and risks that need to be addressed in order to protect card data when using mobile devices, such as smart phones and tablets, to accept payments.

Juniper Research predicts mobile transactions will hit $1.3 trillion worldwide by 2015, four times what it is today, as more and more businesses turn to consumer electronic handheld devices (eg; smart phones, tablets or PDAs) for payment acceptance. As these devices are not solely used as point of sale tools but also to carry out other functions, they introduce new security risks. By design, almost any mobile application could access account data stored in or passing through the mobile device.

The new guidance for merchants focuses on these scenarios and specifically the payment software that operates on these devices. The *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users* leverages industry best practices to educate merchants on what is needed to isolate and prevent card data from exposure.

“Even with rapid adoption of mobile technology in payments, security still tops concerns for merchants. It comes down to the basic element of trust. Consumers want to have confidence that their information is protected - whether at their favorite restaurant, shopping online or making a purchase using a mobile device in lieu of a traditional POS. Currently, it is challenging to demonstrate a high level of confidence in the security of sensitive financial data in devices that were designed for other consumer purposes. Which is why we encourage merchants to consider encrypting cardholder data securely prior to using mobile devices to process transactions,” said Troy Leach, chief technology officer, PCI Security Standards Council.

The guidance goes hand-in-hand with recommendations the Council published in September 2012 for mobile app developers and device vendors on designing appropriate security controls that provide secure mobile payment acceptance solutions for merchants.

Added Leach, “When considering mobile payment acceptance, merchants need to go in with their eyes open. And that’s what the intent of this guidance is, to help merchants understand the risks so that together with developers and device vendors they can safely implement a solution that will enable mobile commerce to flourish.”

The *PCI Mobile Payment Acceptance Security Guidelines* recognize payment security as a shared responsibility. By providing a high level introduction and overview of the mobile payments space and the security risks of mobile devices, the document outlines the unique, complex and evolving mobile environment that underscores the need for all parties in the payment chain to work together to ensure mobile acceptance solutions are deployed securely.

The guidance is organized around the following key areas and objectives:

- **Objectives and Guidance for the Security of a Payment Transaction** - addresses the three main risks associated with mobile payment transactions: account data entering the device, account data residing in the device, and account data leaving the device
- **Guidelines for Securing the Mobile Device** – provides recommended measures for merchants regarding the physical and logical security of mobile devices used for payment acceptance
- **Guidelines for Securing the Payment Acceptance Solution –** provides guidance for the different components of the payment acceptance solution; including the hardware, software, the use of the payment acceptance solution, and the relationship with the customer

A glossary of terms, chart to help determine responsibility for each best practice, checklist for choosing a mobile solution provider, and further detail on additional risks associated with mobile devices are included as appendices.

The document underscores that until mobile hardware and software implementations can meet these guidelines, the best options for merchants is the use of a PCI-validated, Point-to-Point Encryption (PCI P2PE) solution, as outlined in the *Accepting Mobile Payments with a Smartphone or Tablet* fact sheet.

Merchants can download both the *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users* and the *Accepting Mobile Payments with a Smartphone or Tablet* fact

sheet from the PCI SSC website:
https://www.pcisecuritystandards.org/security_standards/documents.php.

As with all PCI Council information supplements, these are only guidelines and do not supersede or replace any PCI DSS requirements.

In 2013 the Council will continue to collaborate with industry subject matter experts and other standards bodies to explore how card data security can be addressed in an evolving mobile acceptance environment, and whether additional guidance or requirements must be developed.

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: 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