PRESS RELEASE

Media Contacts

Ella Nevill	Melissa Zandman
PCI Security Standards Council	Text 100 Public Relations
+1 (781) 876-6248	+1 (617) 399-4914
enevill@pcisecuritystandards.org	pci@text100.com

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL WIRELESS SPECIAL INTEREST GROUP PUBLISHES NEW GUIDE TO WIRELESS SECURITY

Group Creates PCI DSS Wireless Guideline - Document Offers a "How-to Guide" for Wireless and PCI Data Security Standard

WAKEFIELD, Mass., July 16, 2009 – 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 Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announced the findings of the Council's Special Interest Group (SIG) on Wireless technologies.

The Wireless SIG published an information supplement, *PCI DSS Wireless Guideline (https://www.pcisecuritystandards.org/education/info_sup.shtml)* to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and practical methods and concepts for deployment of secure wireless in payment card transaction environments. As wireless networks have been implicated in past payment card data breaches, a SIG formed to investigate and create specific recommendations to increase the security of wireless implementations in accordance with the PCI DSS, and reduce the potential for wireless to be an entry point in attacks on networks containing card data. The new paper is intended for organizations that store, process or transmit cardholder data that may or may not have deployed wireless LAN (WLAN) technology as well as assessors that evaluate PCI DSS compliance.

The Wireless Special Interest Group was chaired by Doug Manchester, director of product security for VeriFone Holdings, Inc. (NYSE: PAY), and was made up of participants from more than 40 organizations - representing interests from: POS vendors, network security companies to acquiring banks and large merchants - providing another opportunity for the Council's Participating Organizations to give feedback on how technology is interpreted through the filter of the DSS. Industry experts from Capita, The Information Assurance Consortium, McDonald's, Motorola and Unified Compliance Framework greatly facilitated the research and publication of the new guidelines.

The findings of the SIG - presented as the *PCI DSS Wireless Guidelines* - provides the first, highly specific, actionable wireless operational guide for complying with PCI DSS, including:

- Generally applicable wireless requirements: These are requirements that all organizations should have in place to protect their networks from attacks via rogue or unknown wireless access points (APs) and clients.
- Requirements applicable for in-scope wireless networks: These are requirements that all organizations that transmit payment card information over wireless technology should have in place to protect those systems.

Each section of the paper contains a detailed list of requirements for meeting the specifications of the DSS, as well as outlining a bulleted summary of recommendations. The information supplement contains a number of easy to use graphics and flow charts aimed at increasing merchants' understanding of how a wireless environment can impact PCI DSS.

In total, nine applicable requirements are analyzed and summarized with recommendations for implementation. These steps are designed to help organizations meet their security needs and provide guidance to assessors helping organizations meet the requirements of the DSS.

"With the *PCI DSS Wireless Guideline,* our group has investigated and now presents an effective means for organizations to minimize the threat potential of wireless technologies," said Manchester. "This first-ever guide will help all in the payment chain, but particularly merchants, better understand the methods necessary to secure their wireless networks, or totally remove the networks from the scope of the DSS and the payment process."

The Wireless SIG is one of four current SIGs that are focused on elements of the DSS that might be considered challenging, or open to interpretation for those in the payment chain seeking to secure their payment card data. SIGs create actionable support documentation, specific instruction or recommendations in an effort to analyze and address specific industry challenges related to an organization's compliance with specific requirements of the DSS. To date, the four SIGs that have been formed focus on: wireless, scoping, virtualization and pre-authorization. The Wireless Special Interest Group is the first to publish their findings.

"The Special interest Groups are another way in which our Participating Organizations are helping to shape the interpretation and evolution of the Data Security Standards," said Bob Russo, general

manager, PCI SSC. “With the feedback from these groups, we anticipate a better, more specific understanding of the payment environment and further guidance on how organizations can adopt PCI standards to create a more formidable payment card security environment.”

The *PCI DSS Wireless Guideline* can be downloaded at (https://www.pcisecuritystandards.org/education/info_sup.shtml).

For more information about the PCI Security Standards Council or to become a Participating Organization please visit pcisecuritystandards.org, or contact the PCI Security Standards Council at participation@pcisecuritystandards.org.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by fostering broad adoption of the PCI Data Security Standard and other standards that increase payment data security. The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Entry Device (PED) Security Requirements and the Payment Applications Data Security Standard (PA-DSS). Merchants, banks, processors and point of sale vendors are encouraged to join as Participating Organizations.