PRESS RELEASE

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Media Contacts

Glenn R. Boyet	Ella Nevill or Matthew Mors
PCI Security Standards Council	Text 100 Public Relations
+1 (781) 876-6248	+1 (212) 331-8410 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	pci@text100.com

FOR IMMEDIATE RELEASE

PCI SECURITY STANDARDS COUNCIL ISSUES UPDATED SELF ASSESSMENT QUESTIONNAIRE

—Enhanced validation tool helps merchants protect their payment data—

WAKEFIELD, Mass., Feb. 6, 2008 — The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (DSS), PCI PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announced that its updated Self Assessment Questionnaire (SAQ) for merchants and service providers is now available.

The SAQ is an important validation tool primarily used by merchants and service providers to demonstrate compliance with the PCI DSS. This new SAQ is specifically designed to simplify and streamline the assessment process and aid merchants who are not required to have onsite assessment to protect payment card data. "With the introduction of the updated SAQ, merchants will now have a better understanding of the steps necessary to secure their payment data and comply with the PCI DSS," said Bob Russo, general manager, PCI Security Standards Council.

Underscoring the need for continued adoption of the PCI DSS by merchants is a recent report by Javelin Research and Strategy in which 63 percent of consumers believe that merchants and retailers are the least secure among payment transaction stakeholders in protecting account information. [1]

In response to industry feedback, this new SAQ incorporates updates designed to reflect the most recent version 1.1 of the DSS and replaces an earlier version that had been in place since January 2005. The SAQ, version 1.1 is now available at https://www.pcisecuritystandards.org/tech/saq.htm and consists of four unique forms to meet various business scenarios. These four include:

- SAQ A: Addresses requirements applicable to merchants who have outsourced all cardholder data storage, processing and transmission.

[1] Cundiff, Bruce. "Data Breaches and Buyer Behavior: Moving PCI Compliance from Costly Burden to Competitive Advantage," Javelin Strategy and Research, March 2007.

—more—

- SAQ B: Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only.
- SAQ C: Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet.
- SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

Also included on the Council's Website is a set of frequently asked questions and an instruction and guideline document for the SAQ, intended to simplify the process and ensure that merchants and service providers can more easily determine which SAQ is the proper tool for them to use in confirming PCI DSS compliance.

"Issuing the latest self assessment questionnaire is another step the PCI Security Standards Council is taking to ensure that all merchants and service providers have options in determining their compliance strategy," said Russo. "Having multiple SAQs available will streamline the process and make it easier for stakeholders to determine their compliance gaps and take action to ensure full compliance with the Standard."

For More Information:

If you would like more information about the PCI Security Standards Council or would like to become a Participating Organization please visit pcisecuritystandards.org, or contact the PCI Security Standards Council at info@pcisecuritystandards.org.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness 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.

###