PRESS RELEASE

Security Standards Council

Payment Card Industry
Security Standards Council, LLC

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

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

PCI SECURITY STANDARDS COUNCIL PIN ENTRY DEVICE SECURITY REQUIREMENTS PROGRAM EXPANDS TO COVER NEW DEVICES

Unattended Payment Terminals and Hardware Security Modules now tested in Council laboratories

WAKEFIELD, Mass., Apr. 20 , 2009 — The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PCI PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today expanded its PIN Entry Device Security Requirements program to cover two new types of devices; unattended payment terminals (UPTs) and hardware security modules (HSMs).

Unattended payment terminals are an increasingly popular form of conducting payment transactions and are used in a variety of scenarios such as museum and concert ticketing, kiosks, automated fuel dispensers and car parking facilities. Hardware security modules are non-user facing devices used in PIN translation, payment card personalization, data protection and e-commerce.

Both UPT and HSM hardware devices can now undergo a rigorous testing and approval process by Council labs to ensure they comply with the industry standards for securing sensitive cardholder account data at all points in the transaction process. The evaluation process includes the logical and physical security of each product. The Council will also provide a list of approved devices on its website, provide documentation and training for labs evaluating these devices and be the single source of information for device vendors and their customers.

“The Council advocates a multi layered approach to security, based on PCI Standards,” said Bob Russo, general manager, PCI Security Standards Council. “The evolution of our PED Security Requirements Program incorporates a comprehensive testing process for UPTs and HSMs so that all components of these devices will now be tested. We are addressing the

—more—

industry need among vendors and merchants to protect cardholder data in all point-of-sale environments."

For More Information:
Further details on the PCI Security Standards Council's PED program can be found here: https://www.pcisecuritystandards.org/pdfs/PCI_PED_General_FAQs.pdf

The new security requirements and evaluation vendor questionnaires can be found on the PCI SSC website here:
https://www.pcisecuritystandards.org/security_standards/ped/index.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 info@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.

# # #