

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 (617) 399-4915 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	#pci@text100.com

FOR IMMEDIATE RELEASE

PCI SECURITY STANDARDS COUNCIL STRENGTHENS PAYMENT CARD DATA SECURITY BY ADDING ADDITIONAL PAYMENT DEVICES TO EXISTING STANDARDS

—PIN entry device security requirements to include unattended payment terminals and host security modules—

WAKEFIELD, Mass., June 30, 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 announces the addition of two new payment industry device types to the PED program to strengthen cardholder data security. Unattended payment terminals (UPTs) and hardware (also known as host) security modules (HSMs) can now undergo a rigorous testing and approval program to ensure they comply with industry standards for securing sensitive payment card data during any point in the transaction process. The Council also will maintain the list of approved UPTs and HSMs, provide documentation and training for labs evaluating these devices and be a single source of information for device vendors and their customers.

The PED Security Requirements are designed to ensure the security of personal identification number (PIN)-based transactions globally and apply to devices that accept PIN entry. Until now, the requirements focused on traditional point-of-sale devices that operate in an environment that is attended by a merchant, cashier, or sales clerk. UPTs are unattended payment devices that include self-service ticketing machines, kiosks, automated fuel pumps and vending machines. Vendors have been manufacturing and having the encrypting PIN pads (EPPs) that go into UPTs evaluated by approved labs, and the payment card brands have been requiring the use of PCI SSC approved EPPs. Having new and overarching UPT testing requirements will further protect the payment card industry participants.

HSMs are secure cryptographic devices that can be used for PIN translation, card personalization, electronic commerce or data protection and do not include any type of cardholder interface. The addition of UPTs and HSMs into the PCI SSC security testing requirements enables the Council to provide testing laboratories with a streamlined evaluation process for achieving compliance of these cryptographic devices.

“PIN entry devices go well beyond the typical POS terminals we are all familiar with and we are continually expanding into more and more areas,” said Bob Russo, general manager, PCI Security Standards Council. “Any device that processes personal identification numbers is an important link in the transaction chain. By including both UPTs and HSMs in the PED Security Requirements, the Council is re-affirming its commitment to developing additional standards to meet the needs of the industry and to ensure continued safety and security for consumers.”

In addition to the founding card brands, the Council is made up of a variety of payment industry organizations that have the opportunity to contribute to the Council's ongoing development and enhancement of the PCI standards. Manufacturers of UPTs and HSMs are encouraged to join the Council as a Participating Organization. Those that join will have the opportunity to review and provide feedback on the draft requirements and process for testing and certifying that UPT and HSM devices are safe and secure. The Council will issue a final set of requirements and documentation by the end of 2008.

For More Information:

More information on the PCI Security Standards Council and becoming a Participating Organization can be found at www.pcisecuritystandards.org, or contact the PCI Security Standards Council at participation@pcisecuritystandards.org. For more information on the latest in PED Security Requirements visit <https://www.pcisecuritystandards.org/pin/>.

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 International, 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 Application Data Security Standard (PA-DSS). Merchants, banks, processors and point of sale vendors are encouraged to join as Participating Organizations.

###