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

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

PCI SECURITY STANDARDS COUNCIL ADDS PIN ENTRY DEVICE (PED) SECURITY REQUIREMENTS

—The Council Will Manage Security Standard and Streamline Testing Process—

WAKEFIELD, Mass., September 11, 2007 — The PCI Security Standards Council, an independent industry standards body providing management of the Payment Card Industry Data Security Standard on a global basis, today announced it has assumed responsibility for the PIN Entry Device (PED) Security Requirements that were previously administered under the auspices of JCB, MasterCard International and Visa International.

The PED Security Requirements are designed to secure personal identification number (PIN)-based transactions globally and apply to devices that accept PIN entry for all PIN based transactions.

“Adding the PED Security Requirements reinforces and expands our commitment to securing the payment process globally,” said Bob Russo, general manager, PCI Security Standards Council. “The addition of the PED Security Requirements under the PCI Security Standards Council will remove conflicting requirements, simplify the testing process and maintain consistent security measures to improve the overall security of payment transactions.”

With the PED Security Requirements administered by the Council, all founding payment brands will recognize PED certification; streamlining the testing process, reducing costs for vendors, and leading to the proliferation of a wider selection of PED products. PED manufacturers submitting devices for security testing will be able to rely on a single set of requirements, helping ensure cardholder security and providing opportunities for faster deployment. Under the Council’s stewardship, each payment brand will bring its own PED expertise and this, when combined with market feedback from POS and terminal vendors will help strengthen the evolving security of these devices.

Implementation of the PED Security Requirements under the PCI Security Standards Council will happen over the next few months. During this time, all devices previously approved and designated as compliant to the existing PCI PED requirements will automatically be grandfathered into the new program. The Council will be honoring existing compliance agreements, with these devices listed on the PCI Security Standards Council approval list until their current existing approvals expire.

The PCI Security Standards Council will also continue to recognize laboratories previously accepted by JCB, MasterCard International and Visa International for PED security testing.

"The addition of the PED Security Requirements brings a new group of stakeholders into the Council," said Russo. "Point of sale and terminal vendors will join solution providers, payment application vendors and others to contribute to the diversity of the Council. In the future, we will continue to explore assuming additional standards to aid us in our goal to enhance global payment data security."

About the PED Security Requirements

PED Security Requirements are divided into the following categories:

Device Characteristics:

- Physical Security Characteristics
- Logical Security Characteristics

Device Management:

- Device Management During Manufacturing
- Device Management Between Manufacturing and Initial Key Loading

Device characteristics are those attributes of the PED that define its physical and its logical characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a cleartext PIN encryption key.

Device management relates to how the PED is produced, controlled, transported, stored and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

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 fostering broad adoption of the PCI Data Security Standard and other standards that increase payment data security.

Payment Card Industry
Security Standards Council, LLC

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

PRESS RELEASE

Media Contacts

Glenn R. Boyet	Ella Nevill or Matthew Mors
PCI Security Standards Council	Text 100 Public Relations
+1 (617) 876-6248	+1 (212) 331-8410 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	pci@text100.com

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the Data Security Standard. Merchants, banks, processors and point of sale vendors are encouraged to join as Participating Organizations.