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 ISSUES LATEST INFORMATION SUPPLEMENTS TO PCI DATA SECURITY STANDARD

—Clarifications made for Penetration Testing and Code Review and Application Firewall Requirements—

WAKEFIELD, Mass., April 22, 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 the availability of two Information Supplements providing further clarification for PCI DSS requirement 11.3, regarding penetration testing, and Requirement 6.6, regarding application code review and application firewalls. Both of these information supplements provide guidance to help merchants and service providers meet these two requirements in support of their PCI DSS compliance efforts. Both information supplements are now available on the Council's website at https://www.pcisecuritystandards.org/tech/supporting_documents.htm.

These Information Supplements are one of the Council's methods to provide clarification and guidance on the PCI DSS. The Council, in conjunction with the payment card industry and its Participating Organizations – now numbering more than 440 companies from around the globe – utilizes these Information Supplements to assist merchants and service providers to adopt PCI DSS and protect customer cardholder data.

Requirement 11.3 addresses penetration testing, which includes network and application layer testing, as well as controls and processes around the networks and applications. Such testing is invaluable to ensuring that both networks and applications are protected from outside intrusion. The Information Supplement for Requirement 11.3 provides guidance on who can perform penetration testing, what the scope of such testing entails, the frequency of such tests, preparation for these tests, testing methodology and components of testing techniques.

Requirement 6.6, which becomes effective on June 30, 2008, provides two options which are intended to address common threats to cardholder data and ensure that input to web applications from un-trusted environments is fully inspected. The Information Supplement for

—more—

this requirement gives organizations clarification on implementing application code reviews (option one) and/or application firewalls (option two).

The first option for application code review for meeting Requirement 6.6 is now subdivided into four alternatives designed to meet the intent of the requirement. They include:

- Manual review of application source code
- Proper use of automated source code analyzer (scanning) tools
- Manual web application security vulnerability assessments
- Proper use of automated web application security vulnerability assessment (scanning) tools.

The second option for Requirement 6.6 is a Web Application Firewall (WAF) which is a security policy enforcement point positioned between a web application and a client end point. The Information Supplement provides recommended capabilities of a select WAF, additional recommended capabilities for certain environments, additional considerations for organizations implementing a WAF and additional sources of information on Web application security.

"The Council is continually looking to provide the clearest guidance to all in the payments chain on implementing the PCI DSS," said Bob Russo, General Manager, PCI Security Standards Council. "These periodic Information Supplements are created from the varied and critical industry feedback we continue to receive from our stakeholders and are designed to make it easier for organizations PCI DSS projects."

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, where you can also find answers to frequently asked questions, 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 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.

###