PRESS RELEASE

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

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

PCI SECURITY STANDARDS COUNCIL PROVIDES BEST PRACTICES FOR SKIMMING PREVENTION

New Resource Educates Merchants on Payment Terminal Environment Protection

WAKEFIELD, Mass., August 25, 2009 – The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS) today released a new resource to educate merchants regarding security best practices that defend against credit card skimming attacks.

Skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes through payment cards or the payment infrastructure. The guidelines presented in the *Skimming Prevention: Best Practices for Merchants* informational supplement include actionable recommendations for protecting merchant terminals based on established countermeasures identified by the merchant community – physical location and security; terminal and terminal infrastructure security; and staff and service access to payment devices.

Spearheaded by the Council's Pin Entry Device (PED) Working Group, with input from law enforcement and industry experts closest to credit card skimming threats, the suggested guidelines help merchants to:

- Evaluate the risks relating to skimming;
- Understand the vulnerabilities inherent in the use of point-of-sale terminals and terminal infrastructure;
- Assess challenges associated with staff that has access to consumer payment devices;
- Prevent or deter criminal attacks against point-of-sale terminals and terminal infrastructure;
- Identify any compromised terminals as soon as possible and notify the appropriate agencies to respond and minimize the impact of a successful attack.

"In today's heightened threat environment, skimming remains a popular method of data compromise. Merchants can protect their business and their customers by educating themselves on risk, and taking active steps to protect their terminal infrastructure from fraud," said Troy Leach, technical director, PCI

Security Standards Council. "By following the guidelines outlined in this document, merchants can improve security levels in their terminal environment and defend against this type of attack. "

In addition to guidance on areas of vulnerability to address, the document provides a series of visual examples of compromised terminals and infrastructure that clarify for merchants exactly the types of warning signs they should be looking for. The new resource also provides practical templates for implementing recommendations such as conducting a risk assessment for your terminal environment and maintaining a regularly updated inventory of evaluated terminal equipment. The Council is publishing this guide as a direct result of feedback from merchant representatives on the PCI SSC Board of Advisors.

"This Skimming Prevention informational supplement is another excellent example of the Council's ongoing mission to educate merchants on steps they can take to increase the security of cardholder data and decrease risk to their payment data environment.," said Bob Russo, general manager, PCI SSC. "Used in conjunction with the Council laboratory tested and approved PIN Entry Device listings, these guidelines will arm merchants with yet more ammunition against data compromise."

The PCI SSC *Skimming Prevention* paper can be downloaded at https://www.pcisecuritystandards.org/education/info_sup.shtml .
For more information about the PCI Security Standards Council or to become a Participating Organization please visit www.pcisecuritystandards.org, or contact the PCI Security Standards Council at participation@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.