Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL RELEASES SUPPLEMENTAL GUIDANCE FOR PROTECTING TELEPHONE-BASED PAYMENT CARD DATA

—New resource helps merchants and service providers understand and implement PCI DSS requirements for voice recordings—

WAKEFIELD, Mass., March 18**,** 2011 —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 Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today released an educational resource on PCI DSS requirements for securing cardholder data in audio recordings. The *Protecting Telephone-Based Payment Card Data Information Supplement* provides actionable recommendations to merchants and service providers for securely processing payment card data over the telephone.

The PCI Security Standards are designed to protect payment card data within merchant and service provider environments and require appropriate measures to protect any systems that store, process and/or transmit cardholder data. Along with face to face or ecommerce environments, the PCI Standards apply to organizations with call center operations where credit card information processed over the phone may be recorded and stored, exposing cardholder data to potential risk.

The Council developed the information supplement to assist merchants and service providers with meeting PCI DSS requirements to secure payment data captured within voice recordings. A product of industry collaboration and stakeholder feedback, the guidance expands upon a PCI Council FAQ published in 2010 and outlines the types of data that are in scope of the PCI requirements for telephone operations. It provides tactics and best practices on how to secure recorded data, with information drawn from resources developed by PCI SSC Board of Advisor member Barclaycard.

—more—

“The interpretation and application of PCI requirements for call recording systems has been a focus for merchants this past year,” said Bob Russo, general manager, PCI Security Standards Council. “Merchants want to know what data they need to protect and how to do it. This new guidance helps them understand the right questions to ask and the steps needed to secure their cardholder data.”

The guidance highlights the key areas that organizations with call center operations need to address in order to process payment cards securely and outlines how best to protect their business and customers from the risks of card data compromise including:

- **Explanation of how PCI DSS applies to cardholder data stored in call recording systems:** Detailed table maps types of data to specific PCI DSS requirements
- **Recommendations for merchants when assessing risk and applicable controls of call center operations:** Contains a quick reference flow chart that provides a step-by-step process for determining necessary controls to meet PCI DSS requirements for voice recordings
- **Specific guidance addressing capture of Sensitive Authentication Data:** Includes suggested methods for rendering data unavailable by query
- **Hints and tips for call centers:** Provides guidance on some of the key considerations faced by call centers when implementing PCI DSS requirements, including specific recommendations and best practices

The new resource serves to promote consistency among merchants, service providers and the assessor community, by providing a common set of best practices for the interpretation and implementation of PCI DSS requirements for the protection of payment card data in call center operations.

Please see the documents library on the PCI SSC website to access the *Protecting Telephone-Based Payment Card Data Information Supplement.*

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 Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors and other vendors are encouraged to join as participating organizations.

###