Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

Laura K. Johnson Lindsay Goodspeed
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

PCI COUNCIL PUBLISHES TOKENIZATION PRODUCT SECURITY GUIDELINES

—Secure tokenization products that reduce storage of payment card data can minimize risk for merchants and acquirers—

SAN FRANCISCO, 2 April 2015— Meeting with acquirers and payment technology leaders today at the TRANSACT15 conference, the PCI Security Standards Council (PCI SSC) announced *Tokenization Product Security Guidelines*. Vendors and solution providers can use the guidance to develop tokenization products that help acquirers and merchants reduce storage of card data in their systems.

Tokenization products devalue payment card data by replacing the Primary Account Number (PAN) with a token. When developed and used securely, these solutions may reduce risk and simplify payment security efforts for merchants by removing the need to store valuable card numbers in their networks and systems. Tokenization products include hardware devices, software applications and service offerings.

Developed in conjunction with a dedicated industry taskforce including technology vendors and security assessors, the *Tokenization Product Security Guidelines* provide technical best practices that address the overall development of tokenization solutions, including:

- Generation of tokens
- How tokens are retained for use (e.g. in back office systems) and stored
- Implementation of products to address potential attack vectors and mitigate associated risks

“Tokenization is one way organizations can limit the locations of cardholder data (CHD). A smaller subset of systems to protect should improve the focus and overall security of those systems, and better security will lead to simpler compliance efforts,” said PCI SSC Chief Technology Officer Troy Leach.

“Minimizing the storage of card data is a critical next step in improving the security of payments. And tokenization does just that,” added PCI SSC General Manager Stephen Orfei. “At the Council, we are excited about the recent advancements in this space. Helping merchants take advantage of tokenization, point-to-point encryption (P2PE) and EMV chip technologies as part of a layered security approach in current and emerging payment channels has been a big focus at this week’s PCI Acquirer Forum. We will continue to collaborate with acquirers and those across the industry to reduce risk and simplify payment security efforts for merchants.”

The *Tokenization Product Security Guidelines* are available on the PCI SSC website at: https://www.pcisecuritystandards.org/security_standards/documents.php

As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover, JCB International, MasterCard and Visa Inc., the Council has 700 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: www.pcisecuritystandards.org.
Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC.