Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

Lindsay Goodspeed
PCI Security Standards Council
+1-781-258-5843
press@pcisecuritystandards.org
Twitter @PCISSC

PCI COUNCIL PUBLISHES PCI DSS DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION

— *Additional Criteria Will Help High Risk Organizations Demonstrate Ongoing Security Efforts For Protecting Payments* —

WAKEFIELD, **Mass.**, 05 June 2015 — Vigilance in maintaining PCI Standards is critical in defending against breaches of cardholder data. Today, the PCI Security Standards Council (PCI SSC) published the *PCI DSS Designated Entities Supplemental Validation* (DESV) to help organizations make payment security part of everyday business practice. The DESV provides additional criteria for demonstrating how PCI DSS controls are being applied continuously to protect payment data from compromise. While specifically designed for entities that may be at greater risk for compromise (for example, those that process or aggregate large amounts of card data), all organizations can benefit from using this tool to ensure ongoing compliance and security throughout the year.

“Locations that aggregate large amounts of cardholder data remain at greater risk of being the target of a focused attack,” said PCI Security Standards Council Chief Technology Officer Troy Leach. “Breach trends continue to point to this, which is why the latest version of the PCI DSS already includes greater stringency around security of dependent services and active monitoring for new threats. The *PCI DSS Designated Entities Supplemental Validation* procedures are not new requirements, but criteria that can help any organization in assessing and documenting how it’s maintaining existing PCI DSS controls on an ongoing basis.”

Unfortunately, some organizations view PCI DSS compliance as a periodic validation exercise only and fail to establish processes to ensure that PCI DSS controls are continuously monitored and applied. According to the *2015 Verizon PCI Compliance Report* that analyzes findings of nearly 3,000 PCI DSS assessments, PCI DSS compliance is generally improving, although just 28.6% of organizations maintained compliance less than a year after a successful validation assessment.

Based on these trends and recent data breaches involving cardholder information, the *PCI DSS Designated Entities Supplemental Validation* is designed to help companies address specific challenges in maintaining ongoing security efforts to protect payments. These include effective compliance program oversight; proper scoping of an environment; and ensuring effective mechanisms are in place to detect and alert on failures in critical security controls.

The payment brands and acquirers will determine which organizations are required to undergo an assessment against the *PCI DSS Designated Entities Supplemental Validation*. Entities should work with their acquiring bank partner to understand any implications for their individual compliance responsibilities.

The *PCI DSS Designated Entities Supplemental Validation* and supporting FAQ are available on the PCI SSC website: https://www.pcisecuritystandards.org/security_standards/documents.php.

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.

***