Media Contact

Lindsay Goodspeed
PCI Security Standards Council
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

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

Payment Card Industry Security Standards Council Enhances Protections for Payment Devices

- Updates Made to Security Standard to Combat Advanced Attacks -

WAKEFIELD, Mass., 9 September 2016 — The PCI Council has updated its payment device standard to enable stronger protections for cardholder data, which includes the PIN (Personal Identification Number) and the cardholder data (on magnetic stripe or the chip of an EMV card) stored on the card or on a mobile device. Specifically, version 5.0 of the PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) Modular Security Requirements emphasizes more robust security controls for payment devices to prevent physical tampering and the insertion of malware that can compromise card data during payment transactions. The updates are designed to stay one step ahead of criminals who continue to develop new ways to steal credit and debit card data from cash machines, in-store and unattended terminals and mobile devices used for payment transactions. Payment devices that directly consume magnetic stripe information from customers remain a top target for data theft, according to the 2016 Data Breach Investigation Report from Verizon.

“Criminals constantly attempt to break security controls to find ways to exploit data. We continue to see innovative skimming devices and new attack methods that put cardholder data at risk for fraud,” said PCI Security Standards Council Chief Technology Officer Troy Leach. “Security must continue to evolve to defend against these threats. The newest PCI standard for payment devices recognizes this challenge by requiring protections against advancements in attack techniques.”

A summary of PCI PTS POI Modular Security Requirements version 5.0 updates are available here and will be discussed in detail with technology and payment security practitioners at the North America PCI Community Meeting in Las Vegas later this month.

The standard and supporting documentation including PCI PTS POI Modular Derived Test Requirements and PCI PTS POI Modular Vendor Questionnaire can be found at: https://www.pcisecuritystandards.org/document_library.

Vendors can begin using PCI PTS POI Modular Security Requirements version 5.0 now for payment device evaluations. Version 4.1 will retire in September 2017 for evaluations of new payment devices.

“With EMV chip the industry is improving protections against skimming and other attacks to reduce fraud,” added PCI Security Standards Council General Manager Stephen Orfei. “But no technology is bulletproof. In this ongoing battle against criminal attacks, we must continue to adapt the way we secure payments. With the latest PCI device standard, PCI is driving the evolution of global industry data security standards that protect payment transactions now and in the future.”

A list of PCI approved devices tested against the PCI PTS POI Modular Security Requirements is available on the PCI Council website for businesses to choose equipment that is verified to protect their customers’ cardholder information in accordance with PCI Standards.

About the PCI Security Standards Council

The PCI Security Standards Council is a 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. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.