

Media Contacts

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

PCI SECURITY STANDARDS COUNCIL UPDATES PCI PIN SECURITY REQUIREMENTS

—Updated version improves clarity and includes testing procedures to ease evaluation—

WAKEFIELD, Mass., December 18, 2014 —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, Card Production Security Requirements and the Payment Application Data Security Standard (PA-DSS), today released v2.0 of the PIN Security Requirements.

The program, aimed at acquiring institutions and agents, contains a complete set of requirements for the secure management, processing and transmission of personal identification number (PIN) data at ATMs, and attended and unattended point-of-sale (POS) terminals. PCI PIN Security Requirements v2.0 was designed to enhance usability and understanding by stating the requirements in a more granular manner.

A noteworthy change is the incorporation of testing procedures into the requirements. This resulted in two versions of the requirements- [PCI PIN Security Requirements v2.0](#) and [PCI PIN Security Requirements and Test Procedures v2.0](#). Including testing producers in a separate version of the document will allow a smoother evaluation and deeper understanding of the requirements.

PIN data continues to be a target for criminals. Examples of common vulnerabilities for PIN theft that the requirements address include:

- PINs that are not protected by use of a secure PIN block
- Failure to use approved cryptographic devices for PIN processing
- Cryptographic keys that are non-random, not unique per POI device, and never change
- Few, if any documented PIN-protection procedures
- Audit trails or logs that are not maintained

To develop and maintain strong technical standards and resources for the protection of payment card data, the PCI Council relies heavily on feedback from its Participating Organizations, including more than 700 of the world's leading merchants, financial institutions and technology and service providers. In July 2014, PCI SSC released a Request For Comment (RFC) seeking input from its Participating Organizations and Qualified Security Assessors on the standing version of the PCI PIN Security Requirements.

"Criminals are actively targeting the point of sale and it's up to us as a community to stop them in their tracks," said Stephen W. Orfei, general manager of the PCI Security Standards Council. "The requirements enhance the protection of devices that accept PINs with the end-goal of securing cardholder data at the POS."

The Council has also published a [Summary of Significant Changes](#) document which provides a high level look at the significant modifications to the requirements.

"With 1.0 we introduced requirements for the secure management, processing and transmission of PIN data at ATMs, and attended and unattended point-of-sale (POS) terminals." said Troy Leach, chief technology officer, PCI Security Standards Council. "Version 2.0 builds on this by improving clarity to ease understanding. The addition of testing criteria will ensure that these products are being tested and validated against the highest level of security."

The PIN Security Requirements are included in the current PTS Security Requirements. The updated program requirements and detailed listing of approved devices are available on the Council's website at:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.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 more than 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: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: <http://www.linkedin.com/company/pci-security-standards-council>. Join the conversation on Twitter: <http://twitter.com/#!/PCISSC>

###