Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

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

Media Contact

Laura K. Johnson
PCI Security Standards Council
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry Security Standards Council Releases Payment Application Data Security Standard Version 3.2

WAKEFIELD, Mass., 27 May 2016 — Today the PCI Security Standards Council (PCI SSC) published a new version of its data security standard for payment software, the Payment Application Data Security Standard (PA-DSS) version 3.2. The Payment Application Data Security Standard is used by payment application vendors to ensure their software products will protect payment card data from theft. Merchants and other businesses globally use "PA-DSS Validated" software to ensure they can safely accept payments, both in-store and online. Using "PA-DSS Validated" software also supports businesses in their efforts to secure payment card data throughout their systems and networks — which is required by the more comprehensive PCI Data Security Standard (PCI DSS).

PA-DSS version 3.2 aligns with the recent release of PCI DSS version 3.2, both of which address growing threats to customer payment information. Updates to standards are based on feedback from the PCI Council's more than 700 global Participating Organizations, as well as data breach report findings and changes in payment acceptance.

"Using secure software and making sure that the software is installed and maintained correctly is a critical part of protecting payments," said PCI Security Standards Council General Manager Stephen Orfei.

Key changes in PA-DSS 3.2 include clarifications to existing requirements and updating requirements to align with PCI DSS v3.2. The revision also makes updates to the detailed instructions included with vendor products (the "PA-DSS Implementation Guide"), which explain how to configure payment applications properly and in accordance with PCI DSS. These address procedures for secure installation of software patches and updates, and instructions for protecting cardholder data if using debugging logs for troubleshooting, as these can be exploited during a compromise.

"We continue to see how failure to properly configure and patch payment applications exposes organizations to attacks that lead to mass data compromise," said PCI Security Standards Council Chief Technology Officer Troy Leach. "That's why in addition to updating PA-DSS to support PCI DSS 3.2, we've added more guidance to help integrators, resellers, and others implementing payment software to configure it properly and protect payment account data."

A full copy of PA-DSS version 3.2, including a Summary of Changes document, Report on Validation (ROV) and Attestation of Validation (AOV) forms are available at: https://www.pcisecuritystandards.org/document_library.

A PCI Perspectives blog post "PA-DSS 3.2: What's New" provides more information on changes to the standard and its supporting documents.

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.

# # #