

Media Contacts

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

PAYMENT CARD INDUSTRY COUNCIL ADVANCES POINT-TO-POINT ENCRYPTION STANDARD

*More Flexible Requirements for Encryption Products Make it Easier
for Merchants to Better Protect Payment Card Data and Reduce Risk of Data Theft*

WAKEFIELD, Mass., 30 June 2015 — Today the Payment Card Industry Security Standards Council (PCI SSC) published an important update to one of its eight security standards, simplifying the development and use of Point-to-Point Encryption (P2PE) solutions that make payment card data unreadable and less valuable to criminals if stolen in a breach.

The updated standard is documented in *PCI Point-to-Point Encryption Solution Requirements and Testing Procedures Version 2.0*. It provides more flexibility to solution providers and to companies that provide P2PE components, services that fulfill specific P2PE requirements and can be integrated into P2PE solutions. In addition to validated P2PE solutions and applications, the PCI Council will now list validated P2PE components, making it easier for a solution provider to create a solution for their merchant customers. Also new with version 2.0, merchants acting as solution providers can implement and manage their own P2PE solutions for their own point-of-sale (POS) locations (Read [P2PE V2 At a Glance](#)).

“Malware that captures and steals data at the point-of-sale continues to threaten businesses and their ability to protect consumers’ payment information. As these attacks become more sophisticated, it’s critical to find ways to devalue payment card data,” said PCI Security Standards Council Chief Technology Officer Troy Leach. “PCI Point-to-Point Encryption solutions help merchants do this by encrypting cardholder data at the earliest point of acceptance, making that data less valuable to attackers even if compromised in a breach.”

Use of a PCI-approved P2PE solution can also allow merchants to reduce where and how the PCI Data Security Standard (called the PCI DSS) applies within their retail environment, increasing security of customer data while simplifying compliance with the PCI DSS (Read [P2PE Merchant Guide](#)).

“Protecting your customers and your corporate brand continue to be the biggest challenges faced by IT executives,” said U.S.-based The HoneyBaked Ham Co.’s VP of Information Technology Bill Bolton. “To meet that challenge, we’ve worked with a P2PE solution provider to adopt a PCI-validated P2PE payment solution across all our stores in a simplified and cost effective way.”

Responding to market feedback from early adopters, now with P2PE v2 merchants have even more options for reducing risk and protecting customer data using encryption. They can manage their own P2PE solutions for their point-of-sale locations, securely separating duties, systems, and functions between merchant encryption (in their retail locations) and decryption environments; or, they can work with a solution provider that will manage a PCI P2PE solution to meet their business needs (Read [P2PE Implementation Case Study](#)).

Added Leach, “With version 2.0 the Payment Card Industry Council is responding to market feedback to provide a simpler approach to validating solutions, while still maintaining a strong level of integrity in the validation process that will result in the most secure options for merchants.”

PCI Point-to-Point Encryption Solution Requirements and Testing Procedures Version 2.0 is available on the [PCI SSC website](#), including [Summary of Changes from P2PE version 1.1.1 to 2.0](#), the [P2PE Instruction Manual \(PIM\) Template](#), and the [P2PE Glossary of Terms, Abbreviations, and Acronyms Version 2.0](#).

For more information on PCI P2PE validated listings, please visit:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php

About the PCI Security Standards Council

The [PCI Security Standards Council](http://www.pcisecuritystandards.org) 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. 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](#).
