

Media Contacts

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

PCI SECURITY STANDARDS COUNCIL POINT-TO-POINT ENCRYPTION PROGRAM HELPS EUROPEAN BUSINESSES PROTECT CUSTOMER DATA

— *As Pressure Mounts on European Organisations to Demonstrate They Are Protecting Their Customers' Personal Information, the Payment Card Industry Pushes Development of Secure Products to Devalue Card Data* —

NICE, France 3 November 2015 — Data security throughout Europe is gaining attention due to an increase in high-profile breaches, record high levels of card-not-present (CNP) fraud and pending legislation from the European Central Bank requiring businesses to demonstrate how they are protecting sensitive consumer information.

To help businesses protect their customers' data, the payment card industry is collaborating to provide Point-to-Point Encryption (P2PE) solutions that make account data unreadable and less valuable to criminals if stolen in a breach. Expanding the availability of these [solutions for merchants](#) is a key priority and focus for payment, security and technology experts convening this week in Nice, France for the annual [PCI Europe Community Meeting](#).

"There are a lot of points where card data can be exposed to criminals as it travels through an organisation's systems and networks. We've seen how hackers use malware and other techniques to steal this data and sell it for use in card-not-present fraud," said PCI Security Standards Council International Director Jeremy King. "Point-to-Point Encryption (P2PE) scrambles card data from the moment it enters your store systems all the way through the transaction cycle. This means it's unreadable and useless to anyone without the proper key to decrypt it. So it secures the original data, and if it is stolen in transit, makes it really difficult for criminals to do anything with it. This would have significantly [devalued the cardholder data](#) stolen in compromises we've seen in recent months."

PCI-validated P2PE products are tested by PCI trained assessors against a peer-reviewed and publically available standard and provide the strongest encryption protections for payment data. The use of a PCI-validated P2PE solution can also cut down on where and how the PCI Data Security Standard (PCI DSS) applies to a merchant's business environment, both increasing security of customer data and simplifying compliance efforts.

European payment security experts from Coalfire, International Payment Services, and the PCI Security Standards Council will share customer case studies and lessons learned from P2PE implementation as part of the agenda at this week's PCI Europe Community Meeting, with a focus on driving further merchant adoption of PCI-validated P2PE solutions throughout Europe and globally.

"We are certainly seeing the adoption of Point-to-Point Encryption gathering pace with merchants across Europe," said International Payment Services' Delia Pedersoli, payment consultant, who will speak at the PCI Europe Community Meeting. "The need for P2PE has become a must have capability for solution providers, as many merchants can see the numerous benefits of adopting this technology within their payments acceptance landscape."

"To help simplify the process and increase availability of validated products and solutions, PCI has recently [released Version 2 of the P2PE standard](#). This provides vendors the flexibility to develop approved components that solution providers can use to more easily develop customized solutions for merchants," said PCI Security Standards Council Director of Certification Programs, Gill Woodcock. "We encourage vendors to take advantage of the newly updated standard to submit their P2PE products for validation and listing on the PCI SSC website."

For more information on PCI P2PE:

- **Merchants:** Visit the PCI SSC website [listing](#) to view available solutions. Check out a quick [case study](#) to learn how other merchants are benefiting from P2PE.

- **Vendors:** Review [P2PE At a Glance](#) for more information on how you can take advantage of the new version of the PCI Point-to-Point Encryption requirements to validate your product.

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.