20th June 2012

European Central Bank
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

To Whom It May Concern:

This letter is a response by the PCI Security Standards Council (PCI SSC) to the European Central Bank's *Recommendations for the Security of Internet Payments*, released in May. The PCI SSC is a global industry standards body focused on securing payment card data that is processed, stored or transmitted regardless of the form factor, device or channel used to initiate payment. Formed in 2006 by the payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to guide the development of open industry standards for global payment security, the PCI SSC has an active base of more than 600 global participating organisations representing leading industry players from the around the world.

ECB and the PCI SSC Share a Similar Objective

The PCI SSC shares a similar goal with the ECB to secure payments made over the Internet. Secure payments underpin financial integrity of the system. Averting card data breaches saves money and prevents disruption for businesses and consumers alike. The importance of this goal rises with the growing volume of Internet-based payments. Because of this importance, the PCI SSC has vigorously engaged in creating and improving global technical standards that secure all card data and accomplish the goal of securing Internet payments. The growth and improvement in payment card security over the past five years has everything to do with global industry involvement in the work of the PCI SSC.

Voluntary Global Collaboration is Driving Stronger Payment Security

It is through the voluntary and active participation of this global community that the PCI SSC sets and develops technical standards and other resources that comprise the essential tools needed to help protect cardholder data against breaches and reduce payment card fraud. Protecting payment card data is a shared responsibility across the payments ecosystem. Together with our industry participants we drive education and awareness of payment security globally.

Today global adoption of the PCI SSC's standards and industry participation in the PCI SSC's process for standards development are at an all-time high. As a result of increased focus on data security and broader implementation of the PCI DSS, today there are fewer large-scale card data breaches in the marketplace.[1] And when breaches do occur, organisations that have applied the PCI SSC's Data Security Standards are in a better position to mitigate the impact of the compromise.[2] Together these industry standards provide the best baseline available for protecting payment card data. Indeed, other industries utilising sensitive data are modelling their own security standards on those developed by the PCI SSC.

[1] Verizon Business 2011. "2011 Data Breach Investigations Report."
[2] The Ponemon Institute. 2011. "2011 PCI DSS Compliance Trends Study."

The ECB's *Recommendations for the Security of Internet Payments* document provides at a high level technical and operational processes. Most if not all of the proposals, both Key Considerations and Best Practises, especially in relation to the use of credit and debit cards for internet payments, are covered in detail by the Requirements and sub requirements of the PCI Data Security Standard. Therefore merchants fully adopting the PCI SSC DSS should meet all the needs of the proposed ECB recommendations. Therefore PCI SSC would like to propose that the ECB document mention that existing applicable standards can be used by all entities to meet the recommendations of the document.

Furthermore, in looking at the document as a whole, whilst the definitions and roles of the various actors within the document are clearly understood by the authors, this may not be the case for all those entities at whom the document is targeted, or other entities reading the document. Therefore providing additional clarity in regard to the actors and their roles would enable all readers to obtain the maximum benefit from the document.

Other Comments

Recommendation BP 5.1 says it is desirable that PSPs require e-merchants who store payment information to have traceability processes in place. Whilst it is beneficial to have traceability for a transaction, the PCI SSC advises merchants to always delete sensitive authentication data after authorisation of a transaction. Alternative methods are available to provide traceability of a transaction without requiring the storage of the PAN, such as the Transaction ID.

Recommendation KC7.5 would appear not to be in full alignment with *BP7.1*. KC7.5 demands PSPs to require e-merchants to support strong authentication, but BP7.1 says that it is only "desirable" that e-merchants support strong authentication.

Recommendation KC11.3 appears to conflict with *BP5.1*. KC11.3 requires PSPs to have e-merchants who store sensitive payment data to deploy measures to protect that data. BP5.1, however, says this deployment is merely "desirable."

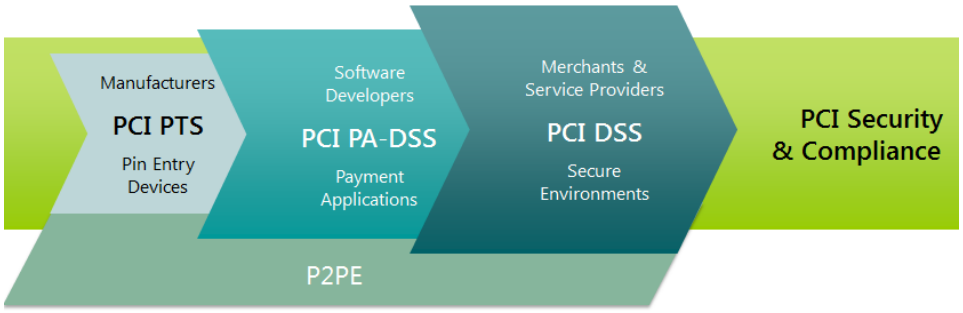
PCI Security Standards Offer the Model to meet the needs of the ECB Guidance

For reasons noted, the global security standards created by the PCI SSC can form the nucleus of efforts by merchants, especially those using credit and debit cards, to meet the needs of the ECB for stronger Internet payment security in the EU.

PCI security standards provide detailed technical and operational requirements to protect cardholder data. The PCI security standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The PCI SSC is responsible for managing these security standards, while compliance with the PCI set of standards is enforced by the Global Card Schemes

PCI SECURITY STANDARDS

tr



Ecosystem of payment devices, applications, infrastructure and users

PCI Security Standards Include:

PCI Data Security Standard (DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. It includes all components used for Internet payments. All entities that accept or process payment cards must comply with the PCI DSS.

PIN Transaction (PTS) Security Requirements

PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC.

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorisation or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC.

Point-to-Point Encryption (P2PE)

The P2PE standard is about cryptographically protecting cardholder data from the point where a merchant accepts the payment card to the point of the merchant's payment processor or acquirer. Even if cardholder data from Internet payments were breached, encryption would render the cardholder data unreadable and ensure its safety. Various aspects of P2PE apply separately to merchants, service providers, and assessors.

Other Resources

Changes to the PCI standards follow a three-year lifecycle; the newest (version 2.0) was published in October 2010. The PCI SSC continuously monitors new threats to cardholder data and may issue information supplements and other guidance for compliance. Examples of focused guidance on emerging issues include mobile, P2PE, virtualisation, wireless, tokenisation, and EMV. Other resources include a web-searchable knowledgebase on payment security, contact information for

approved assessors, education and outreach programs, opportunities for collaboration by participating members, and an active voice in the global payment community.

Collaborating for Stronger Internet Payment Security in the EU/EEA

As the ECB considers its next move on the proposed *Recommendations for the Security of Internet Payments*, The PCI SSC would be pleased to offer any help and support to your team, along with access to our technical resources. Our standards and supporting documents are available in multiple languages on the PCI SSC's website at www.pcisecuritystandards.org.

Please contact me to initiate collaboration between the ECB and the PCI SSC.

Respectfully,

Jeremy King
European Director
PCI Security Standards Council