# Q2 2019 PCI Quarterly Newsletter


## In this issue



## Mastercard

### REMINDERS

*Acquirer and Issuer Compliance*

Mastercard reminds its acquirers and issuers that compliance with the PCI Data Security Standard (DSS) is required. While an acquirer or issuer does not have to report their compliance to Mastercard on an annual basis, an acquirer or issuer must achieve PCI DSS compliance in accordance with Site Data Protection (SDP) Program Standards. Acquirers and issuers must also implement the Mastercard SDP Program by ensuring that their merchants and service providers are compliant with PCI Security Standards. Review section 10.3.1 of the Security Rules and Procedures.

*Merchant and Service Provider Validation*

As part of the SDP Program mandate, PCI compliance validation to Mastercard is required annually for Level 1-3 merchants and Level 1-2 service providers. Mastercard recommends that merchants contact their acquiring bank to determine their level and confirm their compliance validation requirements. Service Providers should review their validation requirements and engage a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV) as necessary. Read What merchants need to know and What service providers need to know.

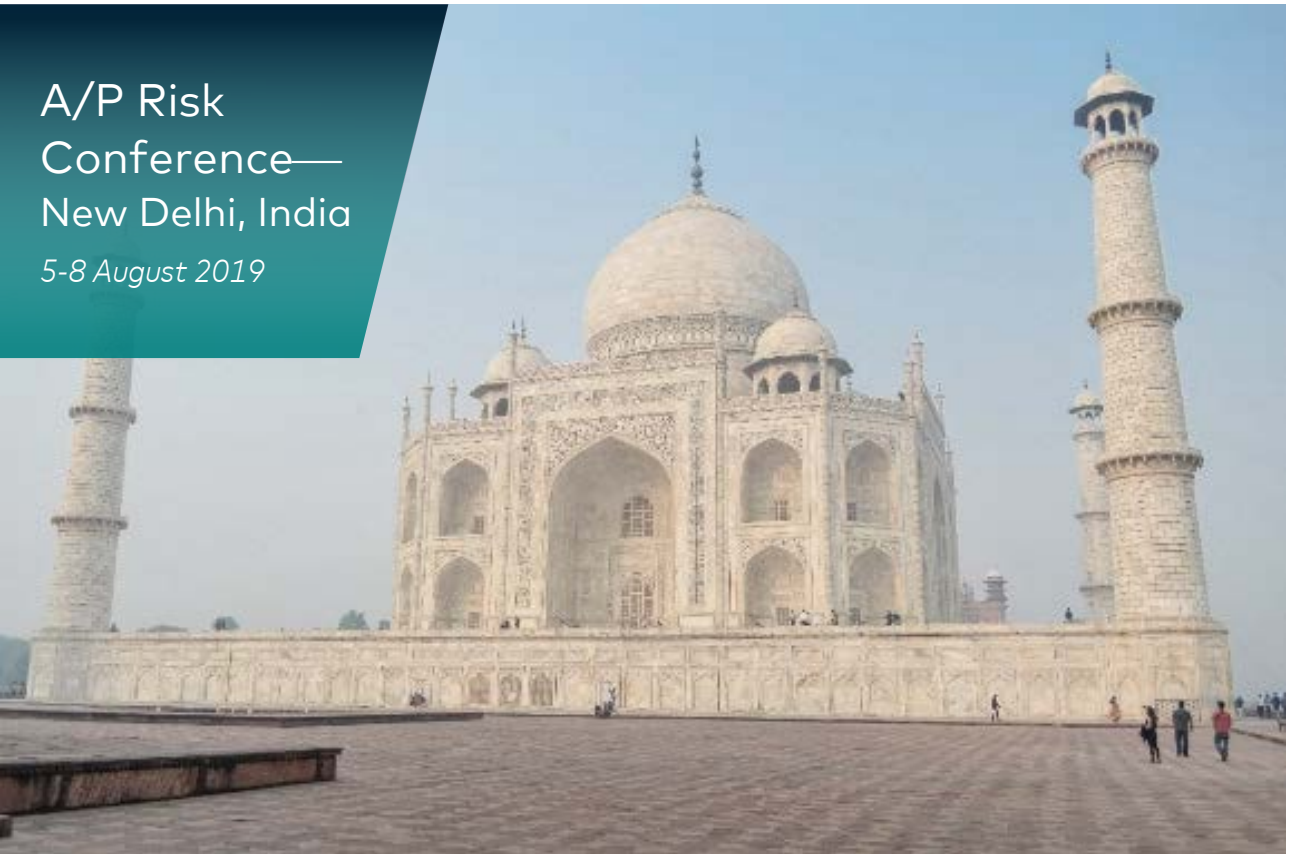
 

*SDP Form due 30 Sept.*
The next SDP Acquirer Submission and Compliance Status Form (SDP Form) for Level 1, Level 2, and Level 3 merchant compliance reporting to Mastercard will be due on 30 September. As a reminder, an acquirer must also certify to Mastercard via the SDP Form that it has a risk management program in place for their Level 4 merchants to identify and manage security risk. For more information on the next SDP Form submission deadline or questions on the Level 4 risk management program certification, acquirers can send an email to sdp@mastercard.com.

*PTS HSM V1 Devices Expired*
PCI approval of devices validated against version 1.0 of the PCI PIN Transaction Security Hardware Security Module (PTS HSM) Requirements expired on 30 April. The PCI Security Standards Council (SSC) has removed PTS HSM V1 devices from the PTS Approval list. This means that PTS HSM V1 devices cannot be newly deployed in the Mastercard network. Devices already deployed may continue to operate until Mastercard announces a sunset date but should be replaced as soon as feasible with an approved version. For questions on PTS devices, send an email to POI_security@mastercard.com.
View the PCI SSC's bulletin.

**EVENTS**
*A/P Risk Conference*
Mastercard's annual Asia Pacific Risk Conference will be held this year at the ITC Maurya on 5-8 August in New Delhi, India. Join the Global Risk Leadership (GRL) team and industry experts who will share the latest updates on intelligence and technology to address the latest cyber threats, the role of Artificial Intelligence in reducing fraud and risk, and biometrics and the importance of digital identity. Do not forget to register for pre and/or post-conference workshops (like the *Mastercard Vendor Seminar* and the *Cybercrime & Payments Security* Workshop) led by subject matter experts. View the agenda.

*Europe Risk Conference*
The annual Europe Risk Conference is taking place at the Rixos Libertas Dubrovnik on 30 September–3 October in Dubrovnik, Croatia.




## MASTERCARD

### NEW MEMBERSHIP

Mastercard has teamed up with the IoT Security Foundation to help refine the rules and standards of IoT so that all transactions happen with the highest level of protection.

Read Securing a Path Forward for IoT by Simon Hunt—EVP Cybersecurity Product Innovation, Mastercard.

### EVENTS

A/P Risk Conference – New Delhi, India 5–8 August

Europe Risk Conference – Dubrovnik, Croatia 30 September-3 October

### PCI 360

Site Data Protection (SDP) Program - Frequently Asked Questions

This document highlights a list of frequently asked questions and answers about the Mastercard SDP Program for acquirers, issuers, merchants, and service providers.

Connect with industry experts and peers for the opportunity to share knowledge and best practices on key payment security issues, vulnerabilities and innovative techniques to mitigate fraud. Learn more about the smartest products and solutions to address fraud and risk in the payments ecosystem. For more information on GRL events including topics covered, send an email to globalrisk@mastercard.com.

## PCI Security Standards Council
## NEWS & UPDATES

*PCI DSS V4.0*

The next major release of the PCI DSS will be version 4. Currently under development, it will incorporate input received from PCI stakeholders during the 2017 request for comments (RFC) period. The next RFC for PCI DSS 4.0 is planned for the second half of the year and will be discussed at the North America, Europe and A/Pacific Community Meetings. Specific timing on the release of the standard will be determined based on feedback received during the development period, but it is not anticipated for publication prior to late 2020. Read PCI DSS: Looking Ahead to Version 4.0.

*SPoC and Contactless Updates*

The PCI SSC recently completed the first of two RFC periods on the draft PCI Contactless Payments on COTS Standard and have a second RFC planned for August. The PCI SSC has also published a Magnetic Stripe Readers (MSR) Annex to the Software-based PIN Entry on COTS (SPoC) Standard which outlines additional security and testing requirements for SPoC Solutions. To learn more about these initiatives and how they support mobile payment acceptance, read PCI on Mobile Payment Acceptance: SPoC and Contactless Updates.

*Software Security Framework Programs*

As part of the PCI Software Security Framework, PCI SSC is in the process of rolling out two new validation programs to support the design, development and maintenance of modern payment software. In the next several weeks, they plan to publish the program documentation, which includes the Software Security Framework Qualification Requirements for Assessors, Secure SLC Program Guide, Secure Software Program Guide and Reporting Templates. Read PCI Software Security Framework: Update on Assessor Qualification and Programs Update: PCI Software Security Framework.

*Card Production Security Assessors*

The PCI SSC is in the process of launching a new program to train and qualify security professionals to perform assessments using the Card Production Security Standards (Card Production and Provisioning Logical Security Requirements and Card Production and Provisioning Physical Security Requirements). The new Card Production Security Assessor (CPSA) Program will create consistency across assessments and ensure guidance and training is aligned with the current threat landscape. The PCI SSC will provide more details about the program in the coming months. Read What to Know About the New Card Production Security Assessor Program.

*Upcoming RFCs/New Process*

Upcoming RFCs on existing and new PCI Security Standards can be found on the RFC page of the PCI SSC website. Since feedback plays a critical role in the ongoing maintenance and development of PCI standards and programs, the PCI SSC has developed detailed and easy-to-understand guidance on its official RFC process. Download the RFC Process Guide or view the RFC-at-a-Glance infographic to learn more about how to participate in RFCs and how feedback from PCI stakeholders is addressed.

## MASTERCARD

PCI 360 *(continued)*

8-Digit BIN Expansion Mandate and PCI Impact

Read how the expansion of 6-digit BINs to 8-digit BINs primarily affects PCI DSS Requirements 3.3 and 3.4.

## PCI COUNCIL

SSC RESOURCES

PCI Firewall Basics

This one-page infographic provides guidance on security basics to help merchants properly configure firewalls.

Glossary of Payment and InfoSec Terms for SMBs

This resource provides small businesses with easy-to-understand explanations of technical terms used in payment security.

Technical PTS and Card Production FAQs


New PIN Transaction Security (PTS) and Card Production FAQs are now available on the PCI SSC website.

**EVENTS**

*Latin America Forum*

The Latin America Forum will be held this year at the Hotel Unique in São Paulo, Brazil on 15 August. Join the PCI SSC for a day of networking opportunities and educational sessions from payment and cybersecurity experts who will discuss challenges and opportunities for data security in Brazil and provide updates on the latest standards and solutions for protecting payments. Registration for the 2019 Latin America Forum is complimentary for all attendees. Simultaneous translation will be available in Portuguese, Spanish, and English. View the agenda here.

*NA and Europe Community Meeting*

Registration is now open for the PCI North America Community Meeting and the PCI Europe Community Meeting.

Do not miss the chance to meet face to face with payment security leaders and other organizations to collaborate, network, learn, and share ideas at these annual PCI Community Meetings. Engaging presentations will arm you with practical strategies, and networking opportunities will allow you to connect with industry leaders in the region. Be sure to check the PCI SSC website to view the agendas that will be announced shortly:

- North America: 17-19 September—Vancouver, BC, Canada
- Europe: 22-24 October—Dublin, Ireland


PCI COUNCIL

EVENTS

Latin America Forum – São Paulo, Brazil 15 August

North America CM – Vancouver, BC, Canada 17-19 September

Europe CM– Dublin, Ireland 22-24 October

TRAINING

The PCI SSC offers a variety of training and re-qualification courses in eLearning and instructor-led formats.

Acquirer Training

Merchant Training

Qualified Integrators & Resellers (QIR) Training

For more information on PCI training courses, send an email to the PCI SSC at training@pcisecuritystandards.org or download Training Programs at a Glance.