Q1 2020 PCI Quarterly Newsletter

Mastercard Cybersecurity Standards & Programs

IN THIS ISSUE

Mastercard

NEWS & REMINDERS

New Security Rules and Procedures Chapter

A new "Cybersecurity Standards and Programs" chapter has been added to the *Security Rules and Procedures* manual. Chapter 2 now provides best practice recommendations for customers to establish and maintain meaningful cybersecurity controls and consolidates existing Payment Card Industry (PCI) compliance programs all under a single chapter. For more information on this change to Mastercard Standards, read *AN 3375—Revised Standards—New Cybersecurity Standards and Programs Chapter* available on Mastercard Connect™.

Cybersecurity Incentive Program (CSIP)

The PCI Data Security Standard (DSS) Risk-based Approach and the PCI DSS Validation Exemption Program are now part of the Mastercard Cybersecurity Incentive Program (CSIP). The CSIP provides eligible merchants using secure technologies such as EMV chip and point-to-point encryption (P2PE) technology increased flexibility within the SDP Standards by either reducing or eliminating compliance validation requirements. The CSIP is optional and currently applies to card-present merchants. See SDP FAQs for more on CSIP programs.

L1-2 Service Provider Validation

As a reminder, annual PCI compliance validation is required for Level 1 and Level 2 Service Providers registered with Mastercard. The PCI Attestation of

Compliance (AOC) must be submitted to pcireports@mastercard.com after initial registration and every year thereafter. If a newly registered service provider is not yet compliant, the PCI Action Plan is required to be completed and submitted for review. For more information on service provider classifications and compliance validation requirements, download the Service Provider Categories and PCI Guidance paper.

PCI Data Security Essentials for SMBs
Mastercard is recommending that acquirers incorporate PCI Data Security Essentials Resources for Small Merchants and the Evaluation Tool into their Level 4 merchant risk management program. These easy-to-understand guidance tools provide security basics for small merchants to protect themselves against payment data theft. *Note—A Level 4 merchant that only completes these tools will not be considered PCI DSS compliant. To validate PCI DSS compliance, an annual Self-Assessment Questionnaire (SAQ) and quarterly network scans must be successfully completed.*

SDP Form due 31 March
The next SDP Form for Level 1, Level 2, and Level 3 merchant PCI DSS compliance reporting is due on 31 March. Acquirers should download the latest version of the form, v5.0, complete it in its entirety and submit it on-time to avoid potential noncompliance assessments for late reporting/non-reporting. For more information on the next SDP Form submission deadline, merchant compliance validation requirements, or questions on the Level 4 risk management program certification, acquirers can send an email to sdp@mastercard.com.

PTS POI v3.x Devices Expire 30 April
PCI approval of devices validated against version 3.0 of the PTS POI Standard expires on 30 April. The PCI Security Standards Council (SSC) will remove the expired v3 devices from the PTS Approval list. This means that PTS POI v3 devices cannot be newly deployed in the Mastercard network after the expiry date. 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.

AML/Sanctions SP Registration 1 May
Effective 1 May, Mastercard will establish a new Service Provider category—Anti-Money Laundering (AML)/Sanctions Service Provider— for third party entities that provide AML and Sanctions related services to customers. An AML/Sanctions Service Provider will be classified as a Level 1 Service Provider under the SDP Program. After initial registration with Mastercard, the AML/Sanctions Service Provider is required to contact the SDP Team and validate their compliance by submitting their PCI DSS AOC.

EVENTS

NAM Cybersecurity & Risk Summit
Mastercard's annual North America Cybersecurity & Risk Summit will be held at The Ritz-Carlton on 1–4 June in Key Biscayne, Florida. Join the Global Risk Leadership (GRL) team and industry experts who will share the latest updates on cyber Intelligence and technology, leveraging strong authentication, the role of Artificial Intelligence in reducing fraud and risk, and establishing high industry standards that benefit stakeholders across the payment ecosystem. Do not forget to register for pre and/or post-conference workshops (like the *Cybersecurity 101 Workshop*) led by subject matter experts. View the agenda.

SDP Acquirer Reporting Deadline
Acquirers uncertain that they will meet the **31 March** PCI DSS merchant compliance reporting deadline due to the coronavirus outbreak (COVID-19) should send an email to the SDP Team to address/resolve your concerns.

MASTERCARD

RESOURCES/PCI 360

Europe SDP Representative

John Elliott has joined the Mastercard Industry Standards team. John will be responsible for driving awareness, understanding, and adoption of security standards for payment security in the Europe region.

Download PCI 360 Educational Resources

ADC Event Management Best Practices

This best practices document highlights how customers and other stakeholders can implement proactive and reactive response strategies to address data compromise events.

EVENTS

Secure the Payments Ecosystem through Innovation and Collaboration

Cybersecurity & Risk Summit-North America Key Biscayne, FL, USA 1–4 June

PCI Security Standards Council

NEWS & UPDATES

PCI DSS v4.0 Draft v0.1 RFC 1

The first draft of the PCI DSS v4.0 Request for Comments (RFC) period is completed. The PCI SSC is currently reviewing the many feedback items received during the first RFC period. PCI stakeholders will have another opportunity to review a second RFC later in 2020. As a reminder, there is still at least a year before the standard is finalized and two years before PCI DSS v4.0 will be required for entities. Stay tuned for further communications on the next RFC period. *Note—v4.0 is a draft only and does not supersede v3.2.1.*

Software-based PIN Entry on COTS Standard v1.1 RFC

The RFC period for the draft Software-based PIN Entry on COTS Standard (SPoC) v1.1 is now open. The PCI SSC is working on a minor revision of the SPoC Standard, including the SPoC Magnetic Stripe Readers (MSR) Annex, mainly to align with the upcoming publication of PCI PTS POI v6.0. The updated security requirements and test requirements will allow SPoC solutions to integrate with PCI PTS Secure Card Reader for PIN (SCRP) devices that support magnetic stripe reads. Participating Organizations (POs), Assessors, Labs, and the Mobile Task Force can submit their feedback comments through the PCI SSC portal.

P2PE v3.0: What Merchants Need to Know

The PCI Point-to-Point Encryption (P2PE) Standard v3.0 was published in December. The latest version simplifies the process for component and solution providers to validate their P2PE products resulting in more solutions to be available in the marketplace. Merchants considering a P2PE Solution are encouraged to use the current

PCI COUNCIL

LATEST RESOURCES

Women in Payments Blog Series

Listen to this blog series to hear women cybersecurity experts discuss their career as well as provide guidance on how to develop a career path in the industry.

PCI DSS for Large Organizations

Download this SIG guidance document to understand how large organizations, the more interconnected and complex, need to evolve their approaches for ensuring awareness of PCI DSS and maintaining compliance.

PCI PIN v3.0 and Card Production FAQs

The updated PTS PIN Security Requirements v3.0 FAQs and Card Production Security Requirements FAQs are now available in the PCI SSC's Document Library.

list of PCI P2PE Solutions on the PCI SSC website and do not need to wait for a P2PE v3.0 validated solution, as solutions validated against v2.0 provide the same level of security assurance. Read What Merchants Need to Know.

PCI SSC/ASC X9 Unified PIN Standard
The PCI SSC and the Accredited Standards Committee X9 Inc. (ASC X9) have completed a joint initiative to create one unified and simplified PIN Security Standard and assessor program for payment card industry stakeholders. The PCI PIN Assessment Working Group (made up of X9, SSC and Payment Brand representatives) collaborated to ensure that the PIN Security Standard satisfies both PCI and X9 requirements. For more information on this initiative, read How Industry Collaboration Created a Unified PIN Standard.

Online Skimming – Growing Threat
Web-based or online skimming attacks continue to be a growing threat to businesses. These attacks steal payment data information by infecting e-commerce websites with malicious code and are difficult to detect. Once a website is infected, payment card information is "skimmed" during a transaction when the customer enters information from their device without the merchant or consumer being aware that the information has been compromised. To learn how merchants and service providers can protect themselves, read Online Skimming and Payment Security.

2020 Brazil Regional Engagement Board
The PCI SSC has announced a new roster of Brazilian payments leaders to serve on its 2020-2021 Brazil Regional Engagement Board. Companies serving on the Board represent leaders from all sectors in the Brazilian payments industry – including vendors, merchants, processors, banks and industry associations. Board members will

A Growing Threat to Businesses—
Online Skimming

Read the bulletin.

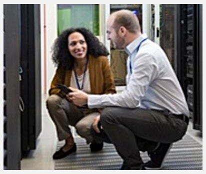
PCI COUNCIL

Get Involved to Make Payments Safer

Join the PCI SSC Participating Organization Program to help secure payment data.

TRAINING

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



Acquirer Training

Acquirers can take a six-hour eLearning training to improve their skill level and provide their merchants with a higher level of advice.

Merchant Training

The PCI SSC offers a range of merchant training and certification programs to support businesses in their payment security efforts.

Qualified Integrators & Resellers (QIR) Training

The QIR course provides guidelines, training and qualification on the most critical control areas related to the installation of payment systems into merchant environments.

Download training FAQs.

act as advisors to the PCI SSC on payment security issues and challenges in the region, and as ambassadors for helping increase education and awareness of standards and best practices for safe payments. Quarterly meetings will be held throughout the year to discuss payment data security issues, trends and market changes. Read the blog.

2020 SIG Topic
Best Practices for Cloud Cryptographic Services has been chosen as the topic for the 2020 Special Interest Group (SIG) project. The SIG will consider the security implications of migrating cryptographic services to the cloud and provide guidance to the industry for the secure operation of these systems applied to payment card transactions. Interested organizations are encouraged to sign up to participate by emailing sigs@pcisecuritystandards.org or can register here.

EVENTS
Community Meetings
The North America, Europe, and Asia-Pacific Community Meetings will take place in Orlando, Florida; Nice, France; and Hanoi, Vietnam this year. Plan on joining the PCI Council to learn about the latest updates and technologies in the payment industry as well as insights and strategies on best practices. Also, hear from engaging keynote speakers and other industry experts.

- 15-17 September: North America Community Meeting in Orlando, Florida, USA
- 20-22 October: Europe Community Meeting in Nice, France
- 11-12 November: Asia-Pacific Community Meeting in Hanoi, Vietnam

India Town Hall—Update
As concerns grow around the spread of the coronavirus outbreak, the PCI SSC has cancelled the India Town Hall Meeting in Mumbai scheduled for next month on 22 April. PCI training classes scheduled on 20-21 April and on 23-24 April will continue to take place as these are smaller events in the region. For updates on upcoming events and trainings including impacts on assessments, visit the PCI SSC's webpage regularly for the latest information. Read PCI SSC Statement on COVID-19.

PCI COUNCIL

EVENTS

Attend a PCI SSC Community Meeting where the SSC staff and industry experts will share the latest payment security updates.

Save the date for 2020 Events.

India Town Hall—Update Mumbai, India
PCI Statement on COVID-19