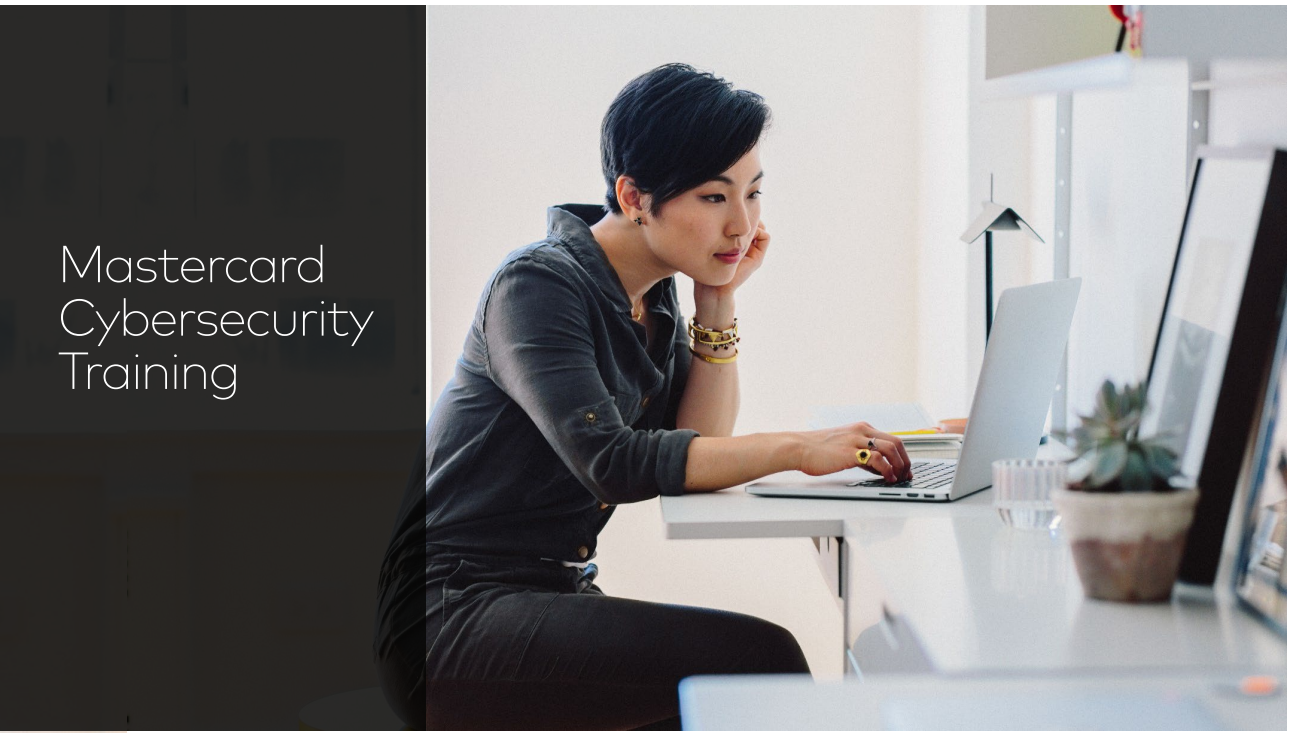
Q3 2020 PCI Quarterly Newsletter



Sign up to receive Mastercard's quarterly newsletter and the PCI Security Standards Council's (SSC) PCI Perspectives blog. Additional PCI information and educational resources can also be found on Mastercard PCI 360 and pcisecuritystandards.org.

Mastercard

NEWS & REMINDERS

Issuer & Merchant Cyber Training

Issuers and merchants can access free online cybersecurity educational training to help maximize their knowledge on defending against cyber attacks. The Issuer Cybersecurity Training offers issuing banks a high-level overview of ATM cash-out attacks and best practices to defend against attacks while the Merchant Cybersecurity Training provides small businesses with an overview of what cybersecurity is, common attack vectors, best practices to implement and what to expect if a data breach occurs. The trainings are available in English, Portuguese and Spanish. Access the trainings here.

Validation Option for L2 Service Providers

Mastercard will be revising SDP Standards to allow an alternative option for qualifying L2 Data Storage Entities (DSEs) to validate compliance. A L2 DSE may submit a PCI PIN Security Requirements Attestation of Compliance (AOC) for Onsite Assessments from a PCI SSC-approved Qualified PIN Assessor (QPA) to the SDP Team instead of the PCI Data Security Standard (PCI DSS) AOC, provided that they do not perform services involving the storage, transmission, or processing of account data.

IN THIS ISSUE

PCI DSS Exemption Program & P2PE
The PCI DSS Compliance Validation Exemption Program offers Level 1 and Level 2 merchants using secure payment technologies such as a validated point-to-point encryption (P2PE) solution an alternative way to validate SDP compliance. Participation in this optional program eliminates the requirement to validate PCI DSS compliance annually. Acquirers are encouraged to work with their merchants to confirm eligibility requirements including the implementation of non-expired P2PE solutions.

PCI PA-DSS Expiration
The Payment Application Data Security Standard (PA-DSS) V3.2 will be expiring in 2022. PA-DSS will be replaced by the PCI Software Security Framework. To help understand and plan ahead for the transition, Mastercard recommends that customers and their merchants and service providers review the PCI SSC's Software Security Framework FAQs document. The resource addresses key questions related to the PCI Software Security Framework, including its impact to PA-DSS validated applications and how PA-DSS will be phased out over time.

PCI 3DS Compliance Reminder
As a reminder, a 3-D Secure Service Provider (3-DSSP) – an organization registered with Mastercard that performs or provides EMV® 3-D Secure (3DS) functions – is required to validate compliance to the SDP Team by submitting their PCI 3DS Core Security Standard AOC. For newly registered 3-DSSPs not yet compliant, the PCI 3DS Prioritized Approach Tool must be completed and submitted for review. *Note—A 3-DSSP's registration will not be deemed complete until compliance with the SDP Program has been validated.*

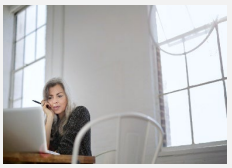
MASTERCARD

LATEST RESOURCES

Free Cybersecurity Assessments

RiskRecon, a Mastercard company, is offering free software-based assessments & consulting through the end of the year to help many industries and regions globally to reduce cybersecurity risk. Enroll here.

Cybersecurity Standards and Programs FAQs



This new PCI 360 document will assist customers, merchants, service providers and card production vendors to answer commonly asked questions about Mastercard's Cybersecurity Standards.

Terminal & PIN Entry Security Standards FAQs

This new FAQs document is designed to help acquirers and merchants with Mastercard security standards applicable to terminals such as ATM and POS terminals, including PIN entry standards.

GVCP Shipping Accommodations Expiration
The Global Vendor Certification Program (GVCP) secure shipping accommodations will expire on 30 September for all GVCP card production vendors affected by the COVID-19 pandemic. This accommodation was extended from June 30 to September 30, 2020 to provide additional flexibility for shipments where secure shipping options have been limited or inhibited. Card production vendors may only use alternate shipping options with issuer authorization. For more information, send an email to gvcp-helpdesk@mastercard.com.

SDP Form due 30 Sept.
The next SDP Form for Level 1, Level 2, and Level 3 merchant PCI DSS compliance reporting to Mastercard is due on 30 Sept. 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 compliance validation requirements or questions on the Level 4 risk management program certification, acquirers can send an email to sdp@mastercard.com.

PCI Security Standards Council

NEWS & UPDATES

PCI DSS v4.0 RFC
PCI SSC has recently concluded the review of over 3,000 comments submitted for the first PCI DSS v4.0 Request for Comments (RFC) last year. This RFC set the record for the most industry submitted comments for a single PCI SSC standard and was the first time the industry had reviewed a working draft of PCI DSS. Another RFC of the draft standard is scheduled for later this year and the final version of the standard is currently planned for completion in mid-2021. For more information about the PCI DSS v4.0 development timeline, read A View into Feedback from the PCI DSS v4.0 RFC.

PCI SPoC v1.1 Available
The SPoC Standard v1.1 is now available on the PCI SSC website. The PCI SSC published a minor revision to the standard to align with the PIN Transaction Security Point-of-Interaction (PTS POI) Standard v6.0 published in June. 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 readers (MSR). This update provides SPoC vendors the option to include a PTS-Approved SCRP that can read contact (chip), contactless, and magnetic-stripe cards securely within a single SPoC solution.

Mobile Payments Standards
PCI SSC is expanding its suite of mobile payment security standards with a new standards effort for contactless on commercial-off-the-shelf (COTS) devices to address PIN acceptance. The effort has the working title of Contactless on COTS with PIN. The new standard will address the native near-field communication (NFC) capabilities and advances in security technology in COTS mobile devices--for example, trusted execution environment (TEE), secure element (SE), secure paths, and trusted application (TA)—that support secure use of screen entry and NFC capture.

PCI PIN & P2PE Security Req. 18-3 Dates
Due to the impact COVID-19 has had on implementations, the PCI SSC has published bulletins updating the effective dates for key block implementations included in PIN and P2PE Security Requirement 18-3: *Encrypted symmetric keys must be managed in structures called key blocks*. The new phased implementation dates are effective immediately and will be reflected in the PCI PIN Security Requirements and Testing Procedures v3.1 due for release later this year, and in a technical FAQ for the time being until the P2PE Standard is updated.

MASTERCARD

EVENT

Virtual Cyber & Risk Summit On-demand

If you missed Mastercard's virtual summit, an InConversation Series event, you can view it on-demand to learn more on the current and future state of cybersecurity in today's hyper-digital environment.

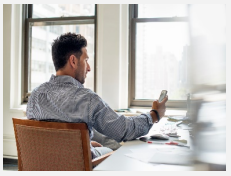
PCI COUNCIL

RESOURCES

Updated Guidance for Non-listed Encryption Solutions

This updated *Information Supplement* provides guidance for merchants using PCI-approved PTS POI device-based account-data encryption solutions that are not listed on the PCI SSC's website.

COVID-19: Protecting Payment Data



The COVID-19 pandemic has quickly changed how many small merchants accept payments. The PCI SSC's resource guide provides tips and educational resources to help small merchants keep their customers' payment data secure.

2021-2022 BOA
The 2021-2022 Board of Advisors nomination period runs from 14 September until 26 October, followed by the election period from 9-20 November 2020. The Board of Advisors represents PCI SSC Participating Organizations worldwide to ensure global industry involvement in the development of PCI security standards. As strategic partners, board members bring industry, geographical and technical insight to PCI SSC plans and projects. For more information on the nomination and election process, review the FAQs.

SIG Proposal
The proposal period for 2021 Special Interest Groups (SIGs) is now open until 21 September 2020. PCI SSC stakeholders are invited to propose ideas for 2021 SIGs. Participating in SIG projects is a great way to share expertise and develop practical payment security resources for the industry. *Note—as the PCI SSC is currently working on PCI DSS v4.0, the 2021 SIG proposals will focus on topics unrelated to the PCI DSS or PA-DSS. This will prevent a SIG from creating guidance that would be associated with a previous version of the PCI DSS.*

TRAINING
eLearning with Online Certification
The PCI SSC has adopted a new eLearning platform to move all informational and certification programs online for the remainder of the calendar year as result of the global COVID-19 pandemic which has affected many in-person testing facilities. To learn more about the new platform, the importance of informational training, and which classes are now available, read the blog: PCI SSC Offers Informational Training via New eLearning Platform.

PCI COUNCIL

RESOURCES (cont.)

Women in Payments Blog Series

Listen to this monthly, award-winning 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.

EVENTS

Online Community Meetings

The 2020 PCI SSC Community Meetings have transitioned from in-person meetings to virtual events. Join the PCI SSC to hear important updates, regional insights, and startling industry reports. Register to attend:

North America CM
6 – 9 October

Europe CM
20 – 23 October

Asia-Pacific CM
4 – 6 November

