SEMIANNUAL PCI NEWSLETTER | NOVEMBER 2024

PCI DSS v4.0.1

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

FEATURED NEWS

PCI DSS v4.0.1

The PCI SSC has published a limited revision to the PCI Data Security Standard (DSS) v4.0 to help address stakeholder feedback and questions received since its release in March 2022. PCI DSS v4.0.1 includes corrections to formatting and typographical errors as well as clarifies the focus and intent of some of the requirements and guidance (refer to the Summary of Changes from PCI DSS v4.0 to v4.0.1). Because this was a limited revision to the standard, there were no new or deleted requirements. In addition, the PCI DSS v4.0.1 Report on Compliance (ROC) Template and Attestations of Compliance (AOC), along with the Self-Assessment Questionnaires (SAQs) and AOCs have also been published and can be found in the PCI SSC Document Library.

Transition to PCI DSS v4.0.1

PCI DSS v4.0 will be retired on 31 December 2024. After that point, PCI DSS v4.0.1 will be the only active version of the standard supported by PCI SSC. Mastercard will continue to accept v4.0 validations until 31 March 2025 provided a merchant or service provider's PCI DSS assessment for compliance validation is completed by the 31 December retirement date. For more information on preparing for version 4.0.1 compliance, visit the Resource Hub.

IN THIS ISSUE

MASTERCARD

RECENT UPDATES

Revised SDP Standards

In May, Mastercard announced several changes to its standards for the Site Data Protection (SDP) Program to support the latest PCI DSS v4.x updates announced by the PCI SSC, add flexibility for customers and their merchants, clarify existing SDP Program requirements, and align with security validation requirements in the industry. These changes included expanding the qualification criteria for the PCI DSS Validation Exemption Program and no longer requiring PCI DSS validation to Mastercard for an acquirer's Level 3 merchants.

Validation Exemption Program Criteria

To recognize the benefits of merchant adoption of secure payment technologies, Mastercard has expanded the Validation Exemption Program's qualification criteria to allow merchants using PCI-listed mobile point-of-sale (MPOS) EMV acceptance solutions to participate in the program. Eligible merchants implementing an MPOS EMV solution that is compliant with the PCI Mobile Payments on Commercial Off-the-Shelf (COTS) (MPoC), PCI Software-based PIN Entry on COTS (SPoC), or PCI Contactless Payments on COTS (CPoC) Standards may be exempt from annually validating its compliance with the PCI DSS.

L3 Merchant Risk Mgmt. Program

An acquirer must now certify to Mastercard that it has a risk management program in place to identify and manage payment security risk within their Level 3 merchant portfolio. This new requirement replaces individual Level 3 merchant reporting on the SDP Acquirer Submission and Compliance Status Form. Level 3 merchants must still comply with the PCI DSS on an annual basis by completing an SAQ, however, validation of compliance to Mastercard is not required.

Mastercard SDP | PCI 360

COMPLIMENTARY EDUCATIONAL RESOURCES

PCI 360 RESOURCES

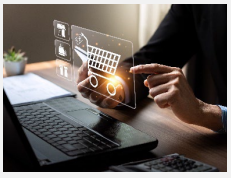
Site Data Protection Program FAQs

Download this Mastercard PCI 360 resource which highlights commonly asked questions about SDP Standards including information on merchant and service provider PCI DSS compliance reporting requirements & acceptable forms of validation.

PCI DSS Validation Exemption Program

Review this updated paper to understand how eligible merchants using approved EMV technology or a PCI-listed solution can begin to participate in Mastercard's Exemption Program, which eliminates the requirement to annually validate PCI DSS compliance.

Overview of a Level 3 Merchant RMP



Read this latest guidance resource intended to assist acquirers with successfully implementing a Level 3 merchant risk management program that meets SDP Program requirements including validating that all merchant URLs have been provided to Mastercard for cyber risk analysis.

PCI SECURITY STANDARDS COUNCIL

LATEST NEWS

Associate Participating Organizations

Join the PCI SSC as an Associate Participating Organization (APO) to help ensure global industry involvement in the development of PCI Security Standards and play an active role in helping to secure the future of payments. There are significant benefits to taking part as an APO including the opportunity to stand for election on the Board of Advisors or serve on Task Forces and Special Interest Groups (SIGs). For more information on becoming an APO, download the infographic or send an email to participation@pcisecuritystandards.org.

Asia-Pacific Community Meeting

Don't miss the opportunity to attend the last PCI SSC Community Meeting of the year. The Asia-Pacific Community Meeting will be held on 20-21 November in Hanoi, Vietnam where attendees can learn about the latest developments in global payment security. Join the Council for engaging sessions that explore the evolving landscape of payment security standards across all facets of the ecosystem and participate in discussions that walk through how key new requirements that were introduced in version 4.0 of the PCI DSS will help strengthen an organization's security posture. View the full agenda here and register today.

Instructor-led Training Opportunities

The PCI SSC operates a variety of programs to train, test, and qualify organizations and individuals who assess and validate compliance to help merchants successfully implement PCI standards and solutions. For those interested in taking a remaining instructor-led training course with the experts from PCI SSC and earn Continuing Professional Education (CPE) credits, check out the schedule of upcoming training opportunities to register or send an email to training@pcisecuritystandards.org.

Associate Participating Organizations

SECURE THE FUTURE OF PAYMENTS TOGETHER

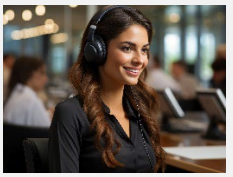
PCI COUNCIL

SSC HIGHLIGHTS

PCI Security Standards Overview Site

Visit this site page to discover the range of PCI Security Standards developed and maintained by the PCI SSC and global payment card industry stakeholders and how the standards define security controls and processes for all entities involved in the payments ecosystem.

Continuing Professional Education



Obtain CPE credits through a variety of opportunities offered by the Council including attending events and training, and through self-study learning by watching videos on the Global Content Library or listening to the Coffee with the Council podcast.

PCI Perspectives Blog

Subscribe to the Council's PCI Perspectives Blog to receive instant notifications delivered straight to your email inbox on the latest industry news, updates, insights, information, and practical resources to help your organization protect payment data.