Q1 2023 PCI Quarterly Newsletter

Revised Standards

Sign up to receive Mastercard's quarterly 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 pcisecuritystandards.org.

Mastercard

REMINDERS

New PCI DSS Compliance Deadlines

In December, Mastercard announced several changes to compliance requirements for compromised entities under the Site Data Protection (SDP) Program. These changes included extending the 60-day PCI Data Security Standard (PCI DSS) compliance deadline to 90 days for all service providers and to 180 days for all merchants after the conclusion of a forensic investigation. Customers should work with their compromised entity to help ensure they achieve full compliance with the PCI DSS on time. Mastercard will no longer approve extension requests for entities that do not meet new PCI DSS compliance deadlines.

SAQ Option for L3-4 ADC Merchants

Effective 1 January 2023, Level 3 and Level 4 merchants that experience an account data compromise (ADC) have the option to validate PCI DSS compliance with either a Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC) conducted by a PCI SSC-approved Qualified Security Assessor (QSA). This change offers smaller compromised merchants increased flexibility to use an alternative validation tool to achieve compliance with no QSA engagement. For more on SAQ validation, send an email to pci_adc@mastercard.com.

SDP Service Provider List
Service providers that are registered with Mastercard and compliant with SDP Program Level 1 service provider requirements are currently listed on the SDP Compliant Registered Service Provider List. The list is complimentary and allows service providers to report their SDP compliance to payments industry stakeholders. Eligible service providers are encouraged to periodically check their status and if not already listed, submit their PCI DSS ROC Attestation of Compliance (AOC) to the SDP Team at pcireports@mastercard.com.

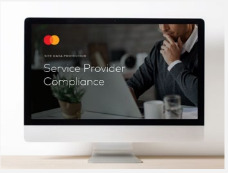
Expired Service Provider Validation
As a reminder, a registered service provider's PCI DSS AOC submission is only valid for one year. To be deemed compliant with the Mastercard SDP Program, it is important that service providers revalidate their compliance on time to remain in good standing and if eligible, listed on the SDP Compliant Registered Service Provider List. Customers are responsible for managing their service providers' compliance and submitting the PCI AOC directly to Mastercard. The My Company Manager application on Mastercard Connect should be updated with a customer's most current security contact information for inquiries the SDP Team may have regarding your service provider's PCI validation. Note—expired validation may lead to escalating noncompliance assessments.

SDP Form due 31 March
The next merchant PCI DSS compliance reporting form for Level 1-3 merchants, compromised merchants, and merchants participating in either the PCI DSS Risk-based Approach or the PCI DSS Compliance Validation Exemption Program is due on 31 March. A new simplified version of the SDP Acquirer Submission and Compliance Status Form (SDP Form), version 6, is available on the Acquirer page of the SDP website and should be used to report the compliance status of an acquirer's merchants. Questions on merchant compliance reporting should be sent to sdp@mastercard.com.

MASTERCARD

HIGHLIGHTS

Service Provider FAQs



Review commonly asked questions about service provider compliance including which registered service provider type must comply with PCI, what their SDP Level is, and how they can be listed on the SDP Compliant Registered Service Provider List.

SDP Compliant Registered Service Provider List

Download the SDP Service Provider List on PCI 360 to choose a Mastercard-approved service provider to help reduce an entity's risk of an ADC event. The list is updated monthly & provides information about a service provider's compliance with the SDP Program.

Acquirer SDP Form v6

This simplified version of the form must be completed by acquirers to report PCI DSS compliance for their L1-3 merchants, semi-annually. Acquirers must also certify on the form they have a L4 merchant risk management program in place to manage payment security risk.

PCI CP & Prov. Standard v2 is Retired
The PCI Card Production and Provisioning Security Requirements v2 expired on 31 December and is now retired. Mastercard will no longer accept version 2 of the standards and validation documents. Only Card Production and Provisioning Security Requirements (Physical and Logical) v3.0.1, which ensures the strongest protections for customer information during card production and provisioning, and the supporting ROCs will be accepted for new PCI assessments. For more information, contact gvcp-helpdesk@mastercard.com or download the FAQs.

PCI PTS POI v4 Devices Expire 30 April 2024
The PCI SSC has extended the expiration date of PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) version 4 devices to 30 April 2024 due to industry feedback regarding global supply-chain disruptions. After this date, PTS POI v4 devices must not be newly deployed in the Mastercard acceptance network. However, version 4 devices in operation/inventory may continue to operate until the end of their business life. For questions on newly deployed devices and/or device replacements, send an email to POI_security@mastercard.com.

PCI Security Standards Council
NEWS & UPDATES

PCI PTS POI Modular Security Reqs. v6.2
The PCI SSC has published a minor revision to the PCI PTS POI Modular Security Requirements that enhance security controls to defend against physical tampering and the insertion of malware that can compromise card data during payment transactions. Version 6.2 of the standard incorporates feedback and comments received via a formal request for comment (RFC) period in Sept. 2022 and modifications in support of the Mobile Payments on Commercial off-the-shelf (COTS) ("MPoC") Security and Test Reqs. View the Summary of Changes here.

PCI MPoC v1.0.1
An updated version of the PCI MPoC standard, v1.0.1, has been published to address minor revisions including errata. The standard was first published last November and is designed to support the evolution of mobile payment acceptance solutions. PCI MPoC builds on the existing PCI Software-based PIN Entry on COTS (SPoC) and PCI Contactless Payments on COTS (CPoC) Standards, which individually address security requirements for solutions that enable merchants to accept cardholder PINs or contactless payments using a smartphone or other COTS mobile device. Read more.

PCI DSS v4: Customized Approach
PCI DSS v4.0 introduced a new method to implement and validate PCI DSS requirements and provide another option for organizations using innovative methods to achieve security objectives. The customized approach was developed in response to stakeholder feedback indicating more flexibility was needed to use innovative technologies to achieve security objectives. To learn more about the customized approach and whether it's right for your organization, the PCI SSC offers guidance that focuses on what to consider when developing and implementing one.

2023-2025 Board of Advisors Election
The 2023–2025 Board of Advisors election period will run from 13–24 March. As strategic leaders who represent all Participating Organizations (PO) worldwide, they bring market, geographical and technical insight to PCI SSC plans and projects. With this year's election, the size and the role of the Board will be expanding to provide a greater range of input for the PCI SSC. For the first time, the Board of Advisors will have the opportunity to vote on new standards and major revisions to standards prior to their release. For more information on the 2023-2025 election process, review the infographic and FAQs.

PCI COUNCIL

SSC HIGHLIGHT

Participating Organization Program

Play a key role in influencing the ongoing development of PCI Security Standards. Join the growing community of POs and play an active part in helping secure the future of payments, globally. Choose from *Principal POs*, *Associate POs*, or *Individual Participants*.

NEW RESOURCES

Global Content Library

Access hours of payment security industry insights such as video content from global community events, covering topics on industry trends, strategies on best practices, and solutions for anyone within the payment ecosystem.

Questions with the Council Video Series

Watch this new video series where the PCI SSC answers payments industry questions about PCI DSS v4. Learn why the standard is more stringent on multi-factor authentication and when organizations should implement new best practice requirements.