



Q3 2023 PCI QUARTERLY NEWSLETTER

Data Security Standard v4



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 at pcisecuritystandards.org.

FEATURED NEWS

Transition to PCI DSS v4

The PCI Data Security Standard (DSS) v3.2.1 [retirement date](#) is quickly approaching. It is important that organizations required to comply with the PCI DSS begin planning and prioritizing work accordingly to ensure a smooth and efficient transition occurs. Mastercard will continue to accept v3.2.1 validations until 30 June 2024 provided an entity's PCI DSS assessment for compliance validation with version 3.2.1 is completed by the 31 March 2024 retirement date. The

additional 3-month grace period will allow extra time for QA and other wrap-up processes to be completed. For more information on transitioning to v4, read: [8 Steps to Take Toward PCI DSS v4](#).

New PCI DSS v4 Resources

The PCI SSC has recently published new resources to help the industry with the transition to PCI DSS v4. These [resources](#) include the updated Self-Assessment Questionnaire (SAQ) Instructions and Guidelines and a new SAQ for Software-based PIN Entry on commercial off-the-shelf (COTS) solutions (SPoC). In addition, the [Items Noted For Improvement \(INFI\) Worksheet](#) has been published to identify and document areas in an organization's environment that need improvement. For additional v4 resources, visit the [Hub](#).

IN THIS ISSUE

FEATURED NEWS

- Transition to PCI DSS v4
- New PCI DSS v4 Resources

MASTERCARD

NEWS & REMINDERS

- Individual PCI Assessor Rotation Best Practice
- Service Provider Registration & PCI
- PCI DSS DESV Best Practice
- SDP Service Provider List
- SDP Acquirer Reporting due 30 Sept.
- PCI DSS Exemption Program Participation

RESOURCES

- Service Provider Reg. & PCI FAQs
- Acquirer SDP Form v6

EVENT

- Mastercard riskx

PCI COUNCIL

NEWS & UPDATES

- PCI 3DS Core & SDK Standards v2
- PCI Secure SLC Standard v1.1 RFC Deadline
- PO Program Benefits

SSC HIGHLIGHT

- Global Content Library

EVENTS

- Community Meetings
- LinkedIn Live

NEWS & REMINDERS

Individual PCI Assessor Rotation Best Practice

A new [best practice](#) for ensuring higher-quality PCI assessments has been added to section 2.1.1, Payment Card Industry (PCI) Security Standards, of the [Security Rules and Procedures](#). Mastercard is recommending that entities required to employ a [PCI SSC assessor](#) for PCI compliance validation rotate the individual assessors they engage from within independent security organizations, as a best practice. Entities are encouraged to review, implement, and explore this best practice when validating their adherence to applicable PCI Security Standards.

Service Provider Registration & PCI

Customers are required to register each service provider that will support any [Mastercard Program Service](#) on their behalf. In addition, a customer's service provider that performs services involving the storage, transmission, or processing of cardholder data must demonstrate compliance with all applicable PCI Security Standards in accordance with the [Site Data Protection \(SDP\) Program](#). Because, a service provider's PCI validation is only valid for one year, it is important that they revalidate their PCI compliance annually and on time.

PCI DSS DESV Best Practice

Mastercard recommends that all service providers demonstrate compliance with the [Designated Entities Supplemental Validation \(DESV\)](#) appendix of the PCI DSS as a best practice, regardless of SDP Level or status. [Compliance](#) with the DESV helps entities assess and document how they are maintaining PCI controls on a continual basis to protect against an [account data compromise \(ADC\) event](#). If a registered service provider experiences a breach or fails to cooperate in a forensic investigation, the service provider will be required to comply with the DESV under SDP Standards.

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 validation](#) to the SDP Team at pcireports@mastercard.com. A noncompliant service provider that poses a significant risk to the payment system will result in the automatic [delisting](#) from the Mastercard-approved service provider list.

SDP Acquirer Reporting due 30 Sept.

The next [SDP Acquirer Submission and Compliance Status Form](#) (SDP Form) for Level 1, Level 2, and Level 3 merchant PCI DSS compliance reporting to Mastercard is due on 30 September. As a reminder, an acquirer must certify to Mastercard via the SDP Form v6 that it has a security risk management program in place for their Level 4 merchant portfolio. Acquirer questions on PCI DSS [compliance validation requirements](#) or the [Level 4 risk management program certification](#) should be sent to sdp@mastercard.com.

PCI DSS Exemption Program Participation

Merchants using secure technologies such as EMV chip technology, PCI point-to-point encryption (P2PE) [solutions](#) or EMV Payment Tokenization may participate in the [PCI DSS Compliance Validation Exemption Program \(Exemption Program\)](#). The Exemption Program is an optional, global program that eliminates the requirement to annually validate compliance with the PCI DSS. Eligible merchants should first contact their acquiring bank who manages their PCI DSS compliance. Your acquirer will then validate to Mastercard via the semi-annual [SDP Form](#) that all qualification requirements have been met.

RESOURCES

[Service Provider Reg. & PCI FAQs](#)



Read this new [PCI 360](#) resource that highlights commonly asked questions on how to register a service provider with Mastercard, which service provider category must comply with PCI standards, & what to do to become SDP compliant.

[Acquirer SDP Form v6](#)



Acquirers can download and [complete](#) v6 of SDP Form to report the PCI DSS compliance of their L1-3 merchants, ADC merchants, and merchants using secure technologies. Acquirers must also [certify](#) that they have a L4 risk mgmt. program in place.

EVENT

[Mastercard riskx](#)



[Attend](#) the Mastercard riskx summit that will be held on 23-26 October in Barcelona, Spain to connect with global technology leaders that will [discuss](#) the forces reshaping today's digital economy and how it will impact the payments ecosystem.

PCI SECURITY STANDARDS COUNCIL NEWS & UPDATES

PCI 3DS Core and SDK Standards v2

A [Request for Comment \(RFC\)](#) period on the draft PCI 3-D Secure (3DS) Core Security Standard v2, the draft PCI 3DS Data Matrix v2, and the draft PCI 3DS Software Development Kits (SDK) Security Standard v2 is anticipated for the December 2023 – January 2024 timeframe. The PCI SSC is revising both [3DS Standards](#) to address the updated EMVCo 3DS specifications, along with additional stakeholder feedback. The current revision effort is intended to address the new 'Split-SDK' implementations. For more information on the revision efforts for the Standards, read the [blog](#).

PCI Secure SLC Standard v1.1 RFC Deadline

The PCI SSC has [extended](#) the RFC period for the PCI Secure Software Lifecycle (Secure SLC) Standard v1.1 to 15 October. Primary contacts of Principal and Associate Participating Organizations (POs) can still review and provide feedback on the currently

published version of the Standard through the [PCI SSC portal](#). The PCI Secure SLC Standard is one of two standards that are part of the [PCI Software Security Framework \(SSF\)](#). It outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle.

PO Program Benefits

There are significant [benefits](#) to taking part in PCI SSC as a PO. You can play an active role in reducing threats to payment security by influencing/collaborating on the ongoing development of PCI Security Standards and in helping to ensure that these standards are implemented globally to secure payment data. You can also expand your knowledge by staying informed on the latest PCI SSC updates as well as increase your company's visibility in the payments industry. For more information on the levels of participation, view the [infographic](#) or send an email to participation@pcisecuritystandards.org.

PCI COUNCIL

SSC HIGHLIGHT

[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.

EVENTS

[Community Meetings](#)



Join the PCI SSC at the remaining 2023 CMs, which will be held in [Dublin, Ireland](#) on 24-26 Oct. and in [Kuala Lumpur, Malaysia](#) on 15-16 Nov. Learn about the latest PCI updates & technologies in the payments industry while networking with industry colleagues.

[LinkedIn Live](#)



Watch the upcoming PCI SSC LinkedIn Live session on 11 October where they will discuss the latest resources available to secure payment data. If you missed the last session on PCI DSS v4, you could watch the replay on LinkedIn [here](#).

