Site Data Protection Program

Frequently Asked Questions

1 June 2024

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third-party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Contents

Document Purpose

The purpose of this document is to answer commonly asked questions about Mastercard Site Data Protection (SDP) Program Standards.

Reference Document

The ***Security Rules and Procedures*** is available on Mastercard Connect™ for further references (refer to section 2.2 for SDP Program requirements).

Site Data Protection Program

The following list of questions is designed to assist customers, merchants, and service providers with SDP Program compliance requirements.

Q: What are the PCI Security Standards?

PCI Security Standards are technical and operational requirements established by the PCI Security Standards Council (PCI SSC) to act as a minimum baseline to protect account data. The standards apply to all entities that store, process, or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in transactions.

Q: Who is responsible for developing and managing the security standards?

The PCI SSC is responsible for developing and managing the security standards as well as promoting the standards globally. The PCI SSC also provides critical tools needed for the implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

Q: What is the PCI Data Security Standard (PCI DSS) and where can I find supporting documents?

The PCI DSS is a set of comprehensive requirements for enhancing security of payment card account data. It covers technical and operational system components included in or connected to cardholder data. If an entity accepts or processes payment cards, then the PCI DSS will apply.

The PCI DSS and supporting documents are available on the PCI SSC website at www.pcisecuritystandards.org.

Q: Does Mastercard manage PCI DSS compliance requirements and validation?

Yes. Mastercard is responsible for managing PCI DSS compliance requirements, validation of compliance, and tracking and enforcement of compliance.

Q: What other PCI Security Standards does Mastercard require entities to comply with?

A list of PCI Security Standards and compliance requirements applicable to issuers, acquirers, merchants, and service providers can be found in *Table 2.1—PCI Security Standards Documentation and Compliance Requirements and Recommendations* in the *Security Rules and Procedures*.

Q: What is the Mastercard SDP Program?

The Mastercard SDP Program consists of rules, guidelines, best practices, and approved compliance validation tools to foster broad compliance with the PCI Security Standards. The SDP Program is designed to help customers, merchants, and service providers protect against Account Data Compromise (ADC) Events.

Q: Who must comply with the PCI DSS under the SDP Program?

Compliance with the PCI DSS and all other applicable PCI Security Standards is required for all issuers, acquirers, merchants, service providers, and any other person or entity that a customer permits, directly or indirectly, to store, transmit, or process account data.

Q: Which entities are required to validate their PCI DSS compliance to Mastercard?

Only merchants and service providers are required to validate their PCI DSS compliance to Mastercard to be deemed compliant with the Mastercard SDP Program.

Q: Does Mastercard accept PCI DSS compliance certificates as validation?

No. The only documentation recognized for PCI Security Standards validation and accepted by Mastercard are the official documents from the PCI SSC website. Any other form of certificate or documentation issued for the purposes of illustrating PCI compliance are not acceptable for validating compliance to Mastercard.

Q: I am a Mastercard customer. Do I need to validate PCI DSS compliance to Mastercard?

No. While compliance with the PCI DSS is required for all issuers and acquirers, validation of a customer's compliance is not required.

Q: I am an issuer. What do I need to do to meet SDP Program requirements?

To ensure compliance with the Mastercard SDP Program, an issuer must:

- Communicate the SDP Program requirements to each Level 1 and Level 2 service provider and validate the service provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the PCI Self-Assessment Questionnaire (SAQ) or the Report on Compliance (ROC); and
- Submit the annual PCI compliance validation for each Level 1 and Level 2 service provider to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter.

Q: I am an acquirer. What do I need to do to meet SDP Program requirements?

To ensure compliance with the Mastercard SDP Program, an acquirer must:

- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 merchant, and validate the merchant's compliance with the PCI DSS by reviewing the PCI SAQ or the ROC;
- Submit the *SDP Acquirer Submission and Compliance Status Form (SDP Form)* for each Level 1 and Level 2 merchant semi-annually to sdp@mastercard.com. Where required by applicable laws, regulations or a regulator, the acquirer must submit the SDP Form for each Level 3 merchant to sdp@mastercard.com upon request by Mastercard;
- Validate to Mastercard that the acquirer has a risk management program in place to identify and manage payment security risk within the acquirer's Level 3 and Level 4 merchant portfolios;
- Communicate the SDP Program requirements to each Level 1 and Level 2 service provider and validate the service provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the PCI SAQ or the ROC; and
- Submit annual PCI validation for each Level 1 and Level 2 service provider to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter.

Q: I am a merchant. What do I need to do to meet SDP Program requirements?

Mastercard requires Level 1 to Level 4 merchants to comply with the PCI DSS as follows:

- *Level 1 merchants*—must undergo an annual PCI DSS assessment resulting in the completion of a ROC conducted by a PCI SSC-approved Qualified Security Assessor (QSA) or PCI SSC-approved Internal Security Assessor (ISA)
- *Level 2 merchants*—must complete an annual SAQ. Level 2 merchants completing SAQ A, SAQ A-EP or SAQ D must additionally engage a PCI SSC-approved QSA or PCI SSC-approved ISA for compliance validation. Level 2 merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA or PCI SSC-certified ISA to complete a ROC.
- *Level 3 merchants*—must complete an annual SAQ or alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC.
- *Level 4 merchants*—may validate compliance with the PCI DSS by completing an annual SAQ or alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC.

Mastercard does not accept PCI DSS validation documentation sent by a merchant. It is your acquirer who will manage your PCI DSS compliance and report your status directly to Mastercard, as applicable.

Q: I am a service provider. What do I need to do to meet SDP Program requirements?

Mastercard requires registered Level 1 and Level 2 service providers to comply with the PCI DSS and all other applicable PCI Security Standards as follows:

- A Level 1 service provider is any Third Party Processor (TPP), Merchant Payment Gateway (MPG), Staged Digital Wallet Operator (SDWO), Digital Activity Service Provider (DASP), Token Service Provider (TSP), 3-D Secure Service Provider (3-DSSP) or Installment Service Provider (ISP) (regardless of volume); and any AML/Sanctions Service Provider, Data Storage Entity (DSE), or Payment Facilitator (PF) that stores, transmits, or processes more than 300,000 total combined Mastercard and Maestro Transactions annually. Level 1 service providers must validate compliance with the PCI DSS annually, and 3-DSSPs must validate compliance with the *PCI 3DS Core Security Standard* every two years by successfully undergoing a PCI assessment resulting in the completion of a ROC conducted by an appropriate PCI SSC-approved QSA.
- A Level 2 service provider is any AML/Sanctions Service Provider, DSE, or PF that stores, transmits, or processes 300,000 or less total combined Mastercard and Maestro Transactions annually; and any Terminal Servicer (TS). Level 2 service providers must validate compliance with the PCI DSS by successfully completing an annual SAQ.
    - As an alternative to validating compliance with an annual SAQ, a qualifying Level 2 DSE may submit a *PCI PIN Security Requirements* Attestation of Compliance (AOC) from a PCI SSC-approved Qualified PIN Assessor (QPA) every two years.
    - As an alternative to validating compliance with an annual SAQ a TS, if eligible, may submit a completed *Terminal Servicer QIR Participation Validation Form*.

The service provider's PCI AOC must be submitted to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter. If a newly registered service provider is not yet compliant, the *PCI Action Plan* available on the service provider page of the SDP Program website must be completed and submitted for review.

For information on service providers registered with Mastercard who must also comply with PCI, download the *Service Provider Registration & PCI FAQs* document on the Mastercard PCI 360 Educational Program resources website at https://www.mastercard.com/globalrisk/en/resources/pci360.html.

Q: Where can I find Mastercard's PCI compliance requirements for merchants and service providers that have experienced an ADC Event?

Mastercard SDP Standards for compromised entities can be found in section 2.2.6, Mandatory Compliance Requirements for Compromised Entities, in the *Security Rules and Procedures* on Mastercard Connect™.

Q: How do I find PCI SSC-approved organizations and individuals to assess and validate PCI DSS compliance?

PCI SSC-approved organizations and individuals to assess and validate compliance can be found on the PCI SSC website at www.pcisecuritystandards.org/program-listings-overview/.

Q: Are PCI DSS remote assessments conducted by a PCI SSC-approved assessor allowed for merchant and service provider compliance validation?

Yes. PCI DSS remote assessments conducted by a PCI SSC-approved assessor are allowed for merchant and service provider compliance validation.

Q: Does Mastercard require PCI SSC-approved assessors to use the *Remote Assessment Guidelines and Procedures* document published by the PCI SSC when conducting a PCI DSS remote assessment?

No. Mastercard does not require assessors to use the *Remote Assessment Guidelines and Procedures* document published by the PCI SSC when conducting a PCI DSS remote assessment. Where an on-site assessment is not possible, Mastercard recommends as a best practice that assessors utilize the guidance document when preparing for a PCI DSS remote assessment.

Q: Will Mastercard accept a PCI DSS AOC for a merchant or service provider that indicates only a "Partial Assessment" was completed for compliance validation?

No. Mastercard will not accept a PCI DSS AOC for a merchant or service provider that indicates only a "Partial Assessment" was completed for compliance validation.

Q: What is *The Mastercard SDP Compliant Registered Service Provider List*?

The Mastercard SDP Compliant Registered Service Provider List provides information about service providers that are registered with Mastercard and compliant with SDP Program Level 1 service provider requirements. The list is complimentary and is provided solely for the convenience of Mastercard customers.

Mastercard updates the service provider listing monthly, and the list can be found on the Mastercard PCI 360 Educational Program resources website at https://www.mastercard.com/globalrisk/en/resources/pci360.html.

Q: How can I be listed on *The Mastercard SDP Compliant Registered Service Provider List*?

To be listed on *The Mastercard SDP Compliant Registered Service Provider List*, a service provider must be registered by one or more Mastercard customers and must have submitted to pcireports@mastercard.com a copy of their PCI DSS AOC conducted by a PCI SSC-approved QSA. PCI DSS validation to Mastercard is required annually.

A registered service provider that validates compliance with a PCI Security Standard other than the PCI DSS (such as the *PCI PIN Security Requirements*) will not be listed.

Q: Does the entity's name on the PCI validation have to match the service provider's registration name to be listed on *The Mastercard SDP Compliant Registered Service Provider List*?

Yes. The entity's name on the PCI validation (PCI DSS ROC AOC) must match the service provider's registration name to be listed on *The Mastercard SDP Compliant Registered Service Provider List* (a 1:1 match).

Any service provider name change request (such as legal entity name change or adding a d/b/a ("doing business as") must be sent to the Mastercard Service Provider Registration Team.

Q: What is the Mastercard Cybersecurity Incentive Program (CSIP) for merchants?

The Mastercard Cybersecurity Incentive Program (CSIP) provides eligible merchants using secure technologies such as EMV chip technology, a PCI-listed point-to-point encryption (P2PE) solution, a PCI-listed mobile point-of-sale (MPOS) EMV acceptance solution, or EMV payment tokenization increased flexibility within the SDP Standards. The CSIP is a component of the SDP Program and is optional for merchants. The CSIP incentivizes merchant participation by either reducing PCI compliance validation requirements through the Mastercard PCI DSS Risk-based Approach or by eliminating the requirement to annually validate compliance with the PCI DSS through the Mastercard PCI DSS Compliance Validation Exemption Program.

Q: Where can I find eligibility requirements for the *PCI DSS Risk-based Approach* and *PCI DSS Compliance Validation Exemption Program*?

Eligibility requirements for the PCI DSS Risk-based Approach and PCI DSS Compliance Validation Exemption Program can be found in section 2.2.4 Mastercard Cybersecurity Incentive Program (CSIP) in the *Security Rules and Procedures*.

Q: What is Mastercard's ISA mandate for Level 1 merchants?

Mastercard requires that Level 1 merchants successfully complete their annual PCI DSS compliance validation requirements using a PCI SSC-approved QSA or PCI SSC-approved ISA. ISA sponsor companies are organizations that have been qualified by the PCI SSC.

Q: What is Mastercard's mandate for merchants and service providers that use eligible third party-provided payment applications or payment software?

Mastercard requires all merchants and service providers that use third party-provided payment applications or payment software to only use payment applications or payment software listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with either the *Payment Card Industry Payment Application Data Security Standard* or the *Payment Card Industry Secure Software Standard*, as applicable.

Mastercard also recommends that merchants and service providers using third party-provided payment software ensure the payment software vendor complies with the *Payment Card Industry Secure Software Lifecycle Standard*.

Q: Where can I find PCI SSC-listed products and solutions?

PCI SSC-approved products and solutions such as approved devices and payment solutions for use at the point of sale, and point-to-point encryption solutions to protect cardholder data can be found on the PCI SSC website at www.pcisecuritystandards.org/product-solutions-listings-overview/.

Q: In support of adopting the 8-digit International Organization of Standards (ISO) Bank Identification Number (BIN) Standard, what is Mastercard's maximum allowable truncation format to meet PCI DSS Requirement 3.4?

For the purposes of the SDP Program and compliance with the PCI DSS, Mastercard's maximum allowable truncation format to meet PCI DSS Requirement 3.4 is "first 8, any other 4". This applies to all 16-digit Mastercard primary account numbers (PANs) regardless of the BIN length.

Q: Are there fines for entities that are noncompliant with the SDP Program?

Yes. A merchant or service provider that is noncompliant with the SDP Program could be affected by potential SDP noncompliance assessments. Table 2.2—Assessments for Noncompliance with the SDP Program of the *Security Rules and Procedures* details escalating fines for merchants and service providers that are noncompliant with the SDP Program.

Q: Where can I find Mastercard SDP Standards and who can I contact for questions on program requirements?

Mastercard SDP Standards can be found in section 2.2, Mastercard Site Data Protection (SDP) Program, of the *Security Rules and Procedures* on Mastercard Connect™.

Customers, merchants, and service providers with questions about SDP Program requirements should contact the SDP Team at sdp@mastercard.com.

Q: Are there additional PCI resources available?

Yes. The following websites provide educational resources and information to help entities comply with the PCI Security Standards:

- *The PCI 360 Education Program* is a complimentary educational program offered by Mastercard to raise awareness of the PCI Security Standards globally – educating customers, merchants and service providers with the tools and resources they need to meet Mastercard's requirements. PCI 360 resources can be found on the Mastercard Global Risk Leadership website at www.mastercard.com/globalrisk/en/resources/pci360.html.
- *The PCI SSC FAQs Resource Database* is a searchable tool that includes a library of questions and answers on a variety of topics across PCI Security Standards and programs. It is updated regularly to address common questions PCI SSC receives from stakeholders. PCI SSC FAQs can be found on the PCI SSC website at www.pcisecuritystandards.org/faqs.