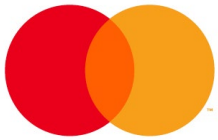

Service Provider Registration & PCI

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 registering service providers with Mastercard who must also comply with applicable Payment Card Industry (PCI) Security Standards in accordance with the Mastercard Site Data Protection (SDP) Program.

Reference Document

Refer to the following reference manuals available on Mastercard Connect™ in the Technical Resource Center (TRC) for information on service provider registration and PCI compliance validation requirements:

- *Security Rules and Procedures*
- *Mastercard Rules*
- *Mastercard Service Provider Registration Guide*

Service Provider Registration & PCI

The following list of questions is designed to assist customers and their agents with registration and PCI compliance validation requirements for service providers.

Q: Is a service provider required to be registered with Mastercard?

Yes. A service provider must be registered with Mastercard before a customer begins to use a service provider to support any of their Mastercard programs.

Q: Who registers a service provider with Mastercard?

Only Mastercard customers may register each service provider that will support any Mastercard Program Service on the customer's behalf.

Q: What happens if a customer does not register a service provider with Mastercard?

Customers that use service providers for Mastercard services without registering such third parties are in violation of the Mastercard Standards.

Q: I am an entity that wishes to become a registered service provider. What do I need to do?

If an entity wishes to become a registered service provider, it must contact each customer on whose behalf it wishes to provide Program Service(s) and request that the customer register the entity as a service provider.

Q: How does a customer register a service provider with Mastercard?

A customer must use the My Company Manager application on Mastercard Connect™ to register a service provider with Mastercard.

Q: How do customers provision a service provider?

A customer must provision a service provider via the Business Administration (BA) tool on Mastercard Connect™.

Q: Where can I find step-by-step instructions on service provider registration and provisioning?

For step-by-step instructions on how to register and provision a service provider, customers can download the *Mastercard Service Provider Registration Guide* available on Mastercard Connect™.

Q: How does Mastercard determine how to categorize a service provider?

Mastercard determines how to categorize a service provider based on the Program Services selected at the time of registration. A service provider may only perform the Program Services it is registered to perform.

Q: Where can I find a list and description of Mastercard service provider classifications?

For a list and description of Mastercard service provider classifications, refer to Chapter 7 of the *Mastercard Rules*, or the "Service Provider Classification" section of the *Mastercard Service Provider Registration Guide* on Mastercard Connect™.

Q: Who should I contact for questions regarding service provider registrations and classifications?

Questions on service provider registrations and classifications should be sent to the Mastercard Service Provider Registration Team at service_provider@mastercard.com.

Q: Are there fees associated with registering a service provider with Mastercard?

Yes. Registration fees are generated upon submission and completion of the customer's registration of each service provider. Renewal fees are charged annually for as long as that customer-service provider relationship continues to exist.

Questions on registration fees and billing should be sent to the Mastercard Service Provider Registration Team at service_provider@mastercard.com.

Q: What if a customer no longer receives Program Services from a registered service provider?

If a customer no longer receives Program Services from a registered service provider, it is recommended that the customer deregister the service provider in Mastercard Connect™.

To deregister a service provider, customers should log on to the My Company Manager [Manage Service Provider] application on Mastercard Connect™.

Q: What type of service provider registered with Mastercard must also comply with applicable PCI Security Standards?

A service provider registered with Mastercard that performs services involving the storage, transmission, or processing of cardholder data and/or related sensitive data governed by PCI must demonstrate compliance with all applicable PCI Security Standards in accordance with the Mastercard SDP Program.

Q: Where can I find Mastercard's PCI compliance requirements for registered service providers?

PCI compliance requirements for registered service providers can be found in section 2.2, "Mastercard Site Data Protection (SDP) Program", of the *Security Rules and Procedures* on Mastercard Connect™ or on the service provider page of the Mastercard SDP Program website.

Q: Who should I contact for questions regarding PCI compliance for registered service providers?

Questions on PCI compliance for registered service providers should be sent to the Mastercard SDP Program Team at pcireports@mastercard.com.

Q: What are Mastercard's SDP Program compliance requirements for customers registering service providers?

To ensure compliance with the Mastercard SDP Program, customers must:

- Communicate SDP Program requirements to each service provider registered with Mastercard that must comply with PCI.
- Validate the registered service provider's compliance with the PCI Data Security Standard (DSS) and any other applicable PCI Security Standard.
- Submit the appropriate PCI compliance validation (PCI Attestation of Compliance [AOC]) for each service provider registered with Mastercard to pcireports@mastercard.com after initial registration and as applicable.

Q: How are registered service providers that must comply with PCI classified under the Mastercard SDP Program?

A registered service provider may be classified as either a Level 1 or Level 2 service provider under the Mastercard SDP Program.

Q: How are service provider levels defined within the Mastercard SDP Program?

A service provider's level within the SDP Program is based on the registered service provider's classification, which is determined by the Mastercard Service Provider Registration Team.

- A Level 1 service provider is any Third Party Processor (TPP), Staged Digital Wallet Operator (SDWO), Digital Activity Service Provider (DASP), Token Service Provider (TSP), 3-D Secure Service Provider (3-DSSP), Merchant Payment Gateway (MPG) 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.

- 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).

Q: What are the PCI compliance requirements for Level 1 service providers?

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 Report on Compliance (ROC) conducted by an appropriate PCI Security Standards Council (SSC)-approved Qualified Security Assessor (QSA).

Q: What are the PCI compliance requirements for Level 2 service providers?

Level 2 service providers must validate compliance with the PCI DSS by successfully completing an annual PCI DSS Self-Assessment Questionnaire (SAQ) D for Service Providers.

Q: Are there alternative validation methods allowed for Level 2 service providers?

Yes. As an alternative to validating compliance with an annual SAQ D for Service Providers, a qualifying Level 2 DSE may submit a PCI PIN Security Requirements AOC from a PCI SSC-approved Qualified PIN Assessor (QPA) every two years; and a TS, if eligible, may submit a completed *Terminal Servicer QIR Participation Validation Form* on an annual basis.

Refer to section 2.2.3, "Service Provider Compliance Requirements", in the *Security Rules and Procedures* for more information about alternative validation methods for Level 2 service providers.

Q: Are Level 1 and Level 2 service providers that have not experienced a confirmed account data compromise (ADC) event required to demonstrate compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI DSS?

No. Level 1 and Level 2 service providers that have not experienced a confirmed ADC event are not required to demonstrate compliance with the DESV appendix of the PCI DSS.

However, Mastercard recommends that registered service providers that must comply with the PCI DSS also demonstrate compliance with the DESV as a best practice to provide greater assurance that PCI DSS controls are being effectively maintained through validation of Business-as-Usual (BAU) processes.

Q: Are Level 1 and Level 2 service providers with a confirmed ADC event required to demonstrate compliance with the DESV appendix of the PCI DSS?

Yes. Level 1 and Level 2 service providers with a confirmed ADC event must demonstrate compliance with the DESV appendix of the PCI DSS.

Refer to section 2.2.6, "Mandatory Compliance Requirements for Compromised Entities", in the *Security Rules and Procedures* for more information.

Q: When should customers submit a registered service provider's PCI validation to Mastercard?

A registered service provider's PCI AOC must be submitted to the Mastercard SDP Program Team after initial registration with Mastercard and every year thereafter unless the service provider is only classified as a 3-DSSP where the PCI 3DS AOC must be submitted every two years.

In addition, the PCI AOC submitted must be for the service provider that performs the actual Program Services it was registered to perform.

Q: Where should PCI validation documents for registered service providers be sent?

PCI validation documents for registered service providers should be sent to the Mastercard SDP Program Team at pcireports@mastercard.com.

Q: What if a customer registers a service provider that is not yet PCI compliant?

If a customer registers a service provider that is not yet compliant, the *PCI DSS Action Plan for Service Providers* or if applicable, the *PCI 3DS Core Action Plan for Service Providers* should be completed and submitted to pcireports@mastercard.com after initial registration.

Both Action Plans are available on the service provider page of the Mastercard SDP Program website.

Q: What if a registered service provider that must comply with PCI does not validate its compliance in accordance with the Mastercard SDP Program?

If a registered service provider that must comply with PCI does not validate its compliance in accordance with the Mastercard SDP Program, the registration of the service provider will not be deemed complete.

Q: Are there fines for registered service providers that are noncompliant with the SDP Program?

Yes. A registered 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 service providers that are noncompliant with the SDP Program.

A service provider's noncompliance also may result in deregistration with Mastercard and/or delisting of a service provider from *The Mastercard SDP Compliant Registered Service Provider List*.

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 updated monthly, is complimentary, and is provided solely for the convenience of Mastercard customers.

Q: Is *The Mastercard SDP Compliant Registered Service Provider List* public?

Yes. *The Mastercard SDP Compliant Registered Service Provider List* is public and can be found on the Mastercard PCI 360 website at www.mastercard.com/pci360.

Q: Is there a fee to be listed on *The Mastercard SDP Compliant Registered Service Provider List*?

No. There is no fee to be listed on *The Mastercard SDP Compliant Registered Service Provider List*. A service provider is added to the listing only after the service provider has been registered by a customer with the Mastercard Service Provider Registration Team and PCI compliance validation for a Level 1 service provider has been received and accepted by the Mastercard SDP Program Team.

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 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 at service_provider@mastercard.com.

Q: Does *The Mastercard SDP Compliant Registered Service Provider List* reflect PCI AOCs past due?

Yes. PCI AOCs that are within 1-90 days past due are listed on *The Mastercard SDP Compliant Registered Service Provider List*. This is not considered a "grace period." Service Providers in respect of whom PCI DSS AOCs are within 1-90 days past due remain listed, and their last AOC dates are represented in yellow (1-60 days past due) or red (61-90 days past due) for ease of identification. After 90 days past due, the registered service provider's name is removed from the List.

Q: What if a registered service provider performs or provides 3DS functions?

A registered service provider that performs or provides 3DS functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification* is required to comply with the PCI 3DS Core Security Standard every two years.

Note—a 3-DSSP required to comply with the PCI DSS must still undergo an annual PCI assessment resulting in the completion of a ROC conducted by a PCI SSC-approved QSA and submit their AOC to Mastercard after initial registration and every year thereafter to be deemed compliant with the SDP Program.

Q: How does a 3-DSSP validate compliance with the Mastercard SDP Program?

Mastercard requires registered 3-DSSPs to comply with SDP Program requirements by performing either of the following:

- Validate compliance with PCI 3DS Core Security Standard Part 1 and Part 2. This would result in one (1) AOC submitted to pcireports@mastercard.com; **OR**
- Validate compliance with PCI DSS and PCI 3DS Core Security Standard Part 2. This would result in two (2) AOCs submitted to pcireports@mastercard.com.

Q: What if a registered service provider uses a 3DS Software Development Kit (SDK)?

A registered service provider that uses any 3DS SDK must validate that each 3DS SDK used is listed on the PCI SSC website as compliant with the PCI 3DS SDK Security Standard.

Q: What if a registered service provider uses a third party-provided payment application or payment software?

A registered service provider that uses third party-provided payment applications or payment software must only use payment applications or payment software listed on the PCI SSC website as compliant with either the PCI Payment Application Data Security Standard (PA-DSS) or the PCI Secure Software Standard, as applicable.

Mastercard also recommends that registered service providers using third party-provided payment software ensure the payment software vendor complies with the PCI Secure Software Lifecycle Standard.

Q: Where can I find additional information on Mastercard SDP Program requirements for registered service providers?

Additional information on Mastercard SDP Program requirements for registered service providers can be found on the PCI 360 resources site at www.mastercard.com/pci360.