MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Overview of a Level 3 Merchant Risk Management Program

JUNE 2024

ACQUIRER CERTIFICATION OF L3 MERCHANT RISK MANAGEMENT PROGRAM

Effective 30 September 2024, acquirers must certify to Mastercard that they have a risk management program in place to identify and manage payment security risk within their Level 3 (e-commerce) merchant portfolio. An additional - yes or no – data field will be added to the updated SDP Acquirer Submission and Compliance Status Form for acquirer certification.

Background

Mastercard Site Data Protection (SDP) Program rules require entities that store, transmit, or process cardholder data, regardless of size, to comply with the Payment Card Industry Data Security Standard (PCI DSS). Merchants with greater than 20,000 but less than or equal to one million total combined Mastercard and Maestro electronic commerce (e-commerce) transactions annually are defined as Level 3 merchants and have been required to validate their compliance to Mastercard to be deemed compliant with the SDP Program.

Acquirers are required to submit the SDP Acquirer Submission and Compliance Status Form (SDP Form) on 31 March and 30 September each year reporting on the PCI DSS compliance validation status of their Level 3 merchants.

Update

On 28 May 2024, Mastercard announced revisions to SDP Program Standards for Level 3 merchant validation requirements, effective 30 September 2024. Under the existing program, acquirers report individual Level 3 merchant PCI DSS validation via the semi-annual SDP Form. Under the revised program, acquirers will now certify to Mastercard that they have a risk management program in place to identify and manage payment security risk within their Level 3 merchant portfolio. An additional - yes or no – data field will be added to the updated SDP Form for acquirers to attest to having a risk management program in place for their Level 3 merchant portfolio. The new data field on the SDP Form must be completed by the acquirer beginning with the 30 September 2024 reporting deadline.

Note—Where required by applicable laws, regulations or a regulator, an acquirer must submit the SDP Form for each Level 3 merchant to sdp@mastercard.com upon request by Mastercard.

Guidance

This overview document contains *minimum requirements* for an acquirer looking to implement a Level 3 merchant risk management program by 30 September 2024. An acquirer's risk management program for Level 3 merchants must meet all the below requirements but may contain more. If an acquirer has an existing risk management program that meets the requirements detailed below, the acquirer is not obligated to change the contents of their current program.

If an acquirer has an existing risk management program that meets the requirements detailed below, the acquirer is not obligated to change the contents of their current program.

Minimum Requirements

When implementing a Level 3 merchant risk management program, an acquirer must ensure that the following elements are included in their program:

- ✓ ***Know who your Level 3 merchants are.***
  A merchant that has greater than 20,000 but less than or equal to one million total combined Mastercard and Maestro e-commerce transactions annually is classified as a Level 3 merchant under the SDP Program.
- ✓ ***Regularly communicate PCI DSS compliance requirements to all Level 3 merchants.***
  This formal communication could be via emails, letters, mailers, newsletters, contracts, account statements, etc.
- ✓ ***Ensure that your Level 3 merchants use only PCI DSS compliant service providers.***
  The Mastercard SDP Compliant Registered Service Provider List is updated monthly and only lists service providers that have been registered with Mastercard and have successfully completed a PCI assessment conducted by a PCI Security Standards Council (SSC)-approved Qualified Security Assessor (QSA).
- ✓ ***Confirm that your Level 3 merchants use PCI compliant payment applications or payment software.***
  Level 3 merchants that use any third party-provided payment applications or payment software must validate that each payment application or payment software used is listed on the PCI SSC website at https://www.pcisecuritystandards.org/product-solutions-listings-overview/ as compliant with either the PCI Payment Application Data Security Standard (PA-DSS) or the PCI Secure Software Standard, as applicable.
- ✓ ***Validate your Level 3 merchants' URL has been provided to Mastercard.***
  Acquirers must ensure merchant URLs are provided to Mastercard as part of the transaction message (refer to *AN 6022 Introduction and Standardization of Transaction Data Elements*). Alternatively, acquirers can provide Level 3 merchant URLs to Mastercard as described in the Mastercard Cyber Secure User Guide on Mastercard Connect™.

Frequently Asked Questions

The following list of questions is designed to assist acquirers with certifying to Mastercard that they have a Level 3 merchant risk management program in place to identify and manage payment security risk.

How has Mastercard changed SDP Program requirements for Level 3 merchant validation?

Effective 30 September 2024, an acquirer must 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.

Does an acquirer still need to report individual Level 3 merchants to Mastercard via the semi-annual SDP Form?

No. An acquirer is no longer required to report individual Level 3 merchants and associated PCI DSS compliance status to Mastercard via the semi-annual SDP Form.

How does an acquirer certify to Mastercard they have a Level 3 merchant risk management program implemented?

An acquirer must certify to Mastercard that they have a Level 3 merchant risk management program in place for their Level 3 merchant portfolio by completing the new - yes or no - data field that will be added to the updated SDP Form.

Are Level 3 merchants still required to comply with the PCI DSS under the SDP Program?

Yes. Level 3 merchants must still comply with the PCI DSS by completing a Self-Assessment Questionnaire (SAQ) or, at their own discretion, engage a PCI SSC-approved QSA to complete a Report on Compliance (ROC).

If an acquirer has an existing Level 3 merchant risk management program that meets the requirements detailed in the "Minimum Requirements" section of this document, do they need to change their current program?

No. If an acquirer has an existing Level 3 merchant risk management program implemented that meets the requirements detailed in the "Minimum Requirements" section of this document, the acquirer is not obligated to change their program.

Does an acquirer have to provide their merchant URLs to Mastercard as a requirement of having a Level 3 merchant risk management program?

Yes. An acquirer must provide their merchant URLs to Mastercard as a requirement of having a Level 3 merchant risk management program implemented.

How do acquirers submit their Level 3 merchant URLs to Mastercard?

Level 3 merchant URLs can be provided to Mastercard as part of the transaction message (refer to *AN 6022 Introduction and Standardization of Transaction Data Elements)* **or** acquirers can provide Level 3 merchant URLs as described in the Mastercard Cyber Secure User Guide on Mastercard Connect™.

Do acquirers have access to Mastercard Cyber Secure™ (Cyber Secure)?

Yes. All acquirers have access to Cyber Secure. Scanning of merchant URLs through Cyber Secure is a service Mastercard is already providing to acquirers as part of their participation to Cyber Secure.

Who can acquirers contact for assistance on Level 3 merchant URL submissions to Mastercard?

Acquirers should contact the Cyber Secure Team at cybersecure@mastercard.com for assistance on Level 3 merchant URL submissions to Mastercard.

For More Information

For more information on Cyber Secure, send an email to cybersecure@mastercard.com.

For more information on an acquirer's Level 3 merchant risk management program, send an email to sdp@mastercard.com. In addition, the following resources are available to you:

The Mastercard SDP Program consists of rules, guidelines, best practices, and approved compliance validation tools to foster broad compliance with the PCI Security Standards.

www.mastercard.com/sdp

The Mastercard PCI 360 Program is a complimentary educational program 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 security requirements.

www.mastercard.com/pci360