MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

PCI DSS Validation Exemption Program for Eligible Merchants Using Secure Technologies

OCTOBER 2018

mastercard

PCI DSS Validation Exemption Program

The Mastercard Payment Card Industry Data Security Standard (PCI DSS) Compliance Validation Exemption Program "Exemption Program" for eligible merchants using secure payment technologies eliminates the requirement to validate PCI DSS compliance annually.

Initially, the Exemption Program was limited to Mastercard and Maestro Level 1 and Level 2 merchants using EMV chip technology. In March 2017, it was expanded to provide greater flexibility within the Site Data Protection (SDP) Program.

The qualification criteria now includes Level 4 merchants and merchants that have implemented point-to-point encryption (P2PE) technology to also participate in the program if they meet all requirements as defined in 10.3.4.2 *Mastercard PCI DSS Compliance Validation Exemption Program* of the Security Rules and Procedures.

Eligibility Requirements

To qualify for the Exemption Program, a merchant must be a Level 1, Level 2, or Level 4 merchant and must satisfy all of the following:

- ✓ Validated PCI DSS compliance within the previous twelve months or has submitted to its acquirer the PCI Security Standards Council (SSC) Prioritized Approach Tool to ensure compliance is achieved within twelve months.
- ✓ Does not store Sensitive Authentication Data.
- ✓ Not been identified by Mastercard as having experienced an Account Data Compromise (ADC) Event during the prior twelve months.
- ✓ Established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements.
- ✓ Satisfied either of the following:
  - At least 75 percent of the merchant's annual total acquired Mastercard and Maestro transaction count is processed through Hybrid POS Terminals; **OR**
  - Implemented a validated P2PE solution listed on the PCI SSC website.

Note—Level 3 merchants are not eligible for the Exemption Program as they are an e-commerce merchant level. The Exemption Program is only applicable to card-present merchants.

Reporting to Mastercard

Acquirers are required to report their Level 1, Level 2, Level 3, and ADC merchants' PCI DSS compliance to Mastercard semi-annually on 31 March and 30 September. The SDP Acquirer Submission and Compliance Status Form addresses PCI compliance reporting for merchants validating compliance with the Mastercard Exemption Program.

To report qualifying Level 1, Level 2, or Level 4 merchants participating in the program, acquirers must complete the Exemption Program data fields on the "PCI Validation Exemption" tab of the SDP Acquirer Submission and Compliance Status Form. On an annual basis, the acquirer will update these data fields attesting that the merchant continues to meet the program's qualification criteria.

Note—Level 4 merchant reporting is optional for merchants that have not had an ADC event or are participating in the Exemption Program.

Maintaining Compliance

Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation to Mastercard is required. The acquirer retains full responsibility for their merchants' PCI DSS compliance and manages all merchant certifications of eligibility for the Exemption Program.

Acquirers may still require PCI compliance validation from a merchant or may accept other forms of evidence of compliance which certifies eligibility for the Exemption Program (for example: a PCI certificate, an acquirer's attestation form, a signed letter from the merchant, etc.). PCI DSS documentation or other information applicable to a merchant's certification of eligibility should be retained for a minimum of five years by the acquirer.

THE EXEMPTION PROGRAM ELIMINATES THE REQUIREMENT TO VALIDATE PCI DSS COMPLIANCE

Applies to:

Asia/Pacific, Europe, Canada, Latin America, Middle East & Africa and US Regions

Merchant Level Eligibility:

Level 1, Level 2, and Level 4 Merchants

Use of Secure Payment Technologies:

EMV Chip

P2PE Solution

SDP Form V5.0

The SDP Form is available on the Acquirer page of the SDP Program website and includes the Mastercard Exemption Program data fields for eligible merchants using EMV chip technology or P2PE technology.

Acquirers should download, complete, and submit version 5.0 of the SDP Form to Mastercard semi-annually on 31 March and 30 September.

Frequently Asked Questions

The following list of questions is designed to assist acquirers and their eligible Level 1, Level 2, and Level 4 merchants using EMV chip technology or P2PE technology on SDP Program Standards for the Mastercard Exemption Program.

Does a merchant need to have implemented both EMV chip and P2PE technologies to be eligible to participate in the Exemption Program?

No. A merchant does not need to have implemented both EMV chip and P2PE technologies. A merchant must either have at least 75 percent annual total Mastercard and Maestro EMV chip transaction counts OR have implemented a validated P2PE solution listed on the PCI SSC website to be eligible to participate in the program.

How can a Level 1, Level 2, or Level 4 merchant apply for the Exemption Program?

Merchants that meet the qualification criteria for the Exemption Program should first contact their acquiring bank who manages their PCI DSS compliance. It is the responsibility of the acquirer to validate that the merchant meets all program requirements and contacts Mastercard at sdp@mastercard.com.

Does the acquirer need to complete an application form for each qualifying merchant?

No. There is no application form to complete for each qualifying merchant.

How does an acquirer report merchants participating in the Exemption Program to Mastercard?

Qualifying merchants must be reported via the SDP Acquirer Submission and Compliance Status Form, semi-annually, on 31 March and 30 September. The acquirer must annually complete the data fields on the "PCI Validation Exemption" tab of the form.

Does a merchant need to validate PCI DSS compliance first to participate in the Exemption Program?

No. A merchant is not required to validate PCI DSS compliance first to participate in the Exemption Program. However, a merchant not yet compliant must submit the PCI SSC Prioritized Approach Tool to its acquirer to ensure compliance will be achieved within twelve months of entering the program. The acquirer will then report to Mastercard the merchant's Prioritized Approach's Milestone 1-6 progress on the "PCI Validation Exemption" tab of the SDP Form.

Where can I find Mastercard's PCI DSS compliance validation requirements for Level 1, Level 2, and Level 4 merchants?

PCI DSS compliance validation requirements for Level 1, Level 2, or Level 4 merchants can be found in section 10.3.4 *Implementation Schedule for Merchants* in the Security Rules and Procedures.

What happens if a merchant already participating in the Exemption Program suffers a confirmed ADC Event?

If a merchant suffers a confirmed ADC Event, they will no longer be able to participate in the program and will be required to validate PCI DSS compliance in accordance with section 10.3.4.3 *Mandatory Compliance Requirements for Compromised Entities* in the Security Rules and Procedures.

Is the Exemption Program applicable to SDP Level 1 or Level 2 Service Providers?

No. This Exemption Program is only applicable to card-present merchants.

For More Information

For more information on PCI DSS Compliance Validation Exemption Program, please send an email to the SDP Program mailbox: sdp@mastercard.com. In addition, the following resources are available to you:

Mastercard

The Mastercard PCI 360 website contains information including white papers and webinars on cardholder data security. This site offers beginner to expert level training curricula suitable for merchants of all sizes and complexity.

Mastercard PCI 360 Education Portal: www.mastercard.com/pci360
Mastercard Site Data Protection Program Site: www.mastercard.com/sdp

The Payment Card Industry Security Standards Council

The PCI SSC's Document Library includes a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.

PCI SSC Document Library: www.pcisecuritystandards.org/document_library
PCI SSC Site: www.pcisecuritystandards.org

PCI 360

For additional frequently asked questions about the Mastercard SDP Program, such as compliance validation requirements for Level 1-Level 4 merchants and appropriate validation tools merchants can use including SAQs, ASV Scans, and On-site Assessments, download the SDP Program- FAQs document on the PCI 360 website.