MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

PCI DSS Validation Exemption Program for Eligible Merchants Using Secure Technologies

MARCH 2021

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.

Since March 2017, the Exemption Program was limited to Mastercard and Maestro card present merchants using either EMV chip technology or a listed PCI point-to-point encryption (PCI P2PE) solution on the Payment Card Industry Security Standards Council (PCI SSC) website. It also required that merchants validate PCI DSS compliance before entering the program or had a plan to achieve compliance within twelve months after entering the program, which created a barrier for most merchants interested in participating.

As a result, to recognize the security benefits of merchant adoption of secure payment technologies, Mastercard has expanded the Exemption Program's qualification criteria to allow card not present merchants using EMV Payment Tokens from Token Service Providers (TSPs) compliant with *Mastercard Token Service Provider Standards* to participate in the Exemption Program. It also no longer requires that merchants validate PCI DSS compliance before entering the program or have a plan to achieve compliance within twelve months after entering the program.

Eligibility Requirements

To qualify for the Exemption Program, a merchant must satisfy all of the following:

- ✓ Does not store Sensitive Authentication Data as defined in the Security Rules and Procedures—2.1 *Cybersecurity Standards*.
- ✓ Not been identified by Mastercard as having experienced an Account Data Compromise (ADC) Event or Potential ADC Event within the previous three years.
- ✓ Has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements.
- ✓ Meets at least one of the following criteria:
  - At least 75 percent of the merchant's annual total acquired Mastercard and Maestro transaction count is processed through Hybrid POS Terminals;
  - Implemented a validated PCI P2PE solution listed on the PCI SSC website; **OR**
  - At least 75 percent of the merchant's annual total acquired Mastercard and Maestro Transaction count is processed using EMV Payment Tokens from TSPs compliant with *Mastercard Token Service Provider Standards*.

Note—As a best practice, Mastercard recommends merchants participating in the Exemption Program validate compliance with the PCI DSS within twelve months of entering the program.

Reporting to Mastercard

The SDP Acquirer Submission and Compliance Status Form (SDP Form) addresses PCI compliance reporting for merchants validating compliance with the Mastercard Exemption Program. Acquirers must complete the Exemption Program data fields on the "PCI Validation Exemption" tab of the SDP Form to report qualifying merchants participating in the program. On an annual basis, the acquirer will update these data fields attesting that the merchant continues to meet the program's qualification criteria.

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 must manage any documentation and/or other information applicable to certification 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: 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

Use of Secure Payment Technologies:

- EMV Chip
- PCI P2PE Solution
- EMV Payment Tokenization

PROGRAM ENHANCEMENTS

Summary of Changes, March 2021—

- Allows qualifying merchants using EMV Payment Tokenization to participate
- Incentivizes both card present and card not present merchant participation
- Eliminates PCI DSS compliance validation requirement (initial/after) for qualifying merchants

mastercard

Frequently Asked Questions

The following list of questions is designed to assist acquirers and their merchants using EMV chip technology, PCI P2PE solutions and EMV Payment Tokenization with SDP Program Standards for the Mastercard Exemption Program.

What is the Exemption Program?

The Exemption Program is an optional, global program that eliminates the requirement for merchants using secure payment technologies to annually validate their PCI DSS compliance.

Which merchants are now eligible to participate in the Exemption Program?

Eligible merchants using secure technologies such as EMV chip technology, PCI P2PE solutions and EMV Payment Tokenization may participate in the Exemption Program. To qualify for the Exemption Program, a merchant must satisfy all eligibility requirements found in section 2.2.4 *Mastercard Cybersecurity Incentive Program (CSIP)* in the Security Rules and Procedures.

How can qualifying merchants 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. The acquirer must annually complete the data fields on the "PCI Validation Exemption" tab of the SDP Form.

Does Mastercard still require that eligible merchants validate PCI DSS compliance before entering the program or have a plan to achieve compliance within twelve months after entering the program?

No. Mastercard no longer requires that eligible merchants validate PCI DSS compliance before entering the program or have a plan to achieve compliance within twelve months after entering the program.

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

PCI DSS compliance validation requirements for Level 1, Level 2, Level 3 and Level 4 merchants can be found in section 2.2.2 *Merchant Compliance Requirements* in the Security Rules and Procedures.

Can a merchant that has been identified by Mastercard as having experienced an ADC Event or Potential ADC Event within the last three years participate in the Exemption Program?

No. If a merchant has been identified by Mastercard as having experienced an ADC Event or Potential ADC Event within the last three years, they cannot participate in the Exemption Program.

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

No. The Exemption Program is only applicable to 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 helps educate customers, merchants and service providers with the tools and resources they need to meet Mastercard SDP Program requirements.

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