MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Validation Exemption Program

APRIL 2025

Background
Mastercard offers merchants using EMV technology, a Payment Card Industry Security Standards Council (PCI SSC)-listed solution, or a suite of cybersecurity and risk management tools the option to participate in the Mastercard Cybersecurity Incentive Program (CSIP). The Mastercard CSIP is a component of the Site Data Protection (SDP) Program and provides qualifying merchants with alternative methods for validating compliance with the PCI Data Security Standard (DSS).

Validation Exemption Program
The Validation Exemption Program (VEP), formerly known as the Mastercard PCI DSS Compliance Validation Exemption Program (Exemption Program), allows a qualifying Level 1, 2, 3, or 4 merchant to be exempt from annually validating its compliance with the PCI DSS if they use approved secure technologies. These include EMV chip technology, a PCI-listed point-to-point encryption (P2PE) solution, a mobile point-of-sale (MPOS) EMV acceptance solution compliant with the PCI Software-based PIN Entry on Commercial Off-the-Shelf (COTS) (SPoC), PCI Contactless Payments on COTS (CPoC), or PCI Mobile Payments on COTS (MPoC) Standards, or EMV payment tokenization.

VEP EXEMPTS A MERCHANT FROM VALIDATING PCI DSS COMPLIANCE

Eligibility Requirements
To qualify for VEP, a Level 1, 2, 3 or 4 merchant must satisfy the following requirements:

- ✓ The merchant does not store sensitive authentication data as defined in the *Security Rules and Procedures*—2.1 *Cybersecurity Standards*.
- ✓ The merchant has not been identified by Mastercard as having experienced an account data compromise (ADC) event or potential ADC event within the previous three years.
- ✓ The merchant has established and annually tests an incident response plan in accordance with PCI DSS requirements.
- ✓ The merchant has satisfied one 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 PCI P2PE solution listed on the PCI SSC website, **OR**
  - Implemented an MPOS EMV acceptance solution such as SPoC, CPoC, or MPoC 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 Token Service Providers (TSPs) compliant with *Mastercard TSP Standards*.

Note—A qualifying merchant may participate in VEP unless a merchant's participation conflicts with applicable law or regulation requiring such compliance and validation. A merchant that does not satisfy VEP's eligibility criteria must continue to validate its PCI DSS compliance annually in accordance with the Mastercard SDP Program.

Maintaining Compliance
Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement. A merchant's acquirer may still require PCI DSS compliance validation from a merchant or may accept other forms of evidence of compliance which certifies eligibility for VEP.

Frequently Asked Questions

The following list of questions is designed to assist acquirers and their merchants using EMV chip technology, a PCI-listed P2PE solution, a PCI-listed MPOS EMV acceptance solution, or EMV payment tokenization with SDP Program Standards for the Validation Exemption Program.

What is VEP?

VEP, formerly known as the Mastercard PCI DSS Compliance Validation Exemption Program (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 eligible to participate in VEP?

Eligible merchants using secure technologies such as EMV chip technology, a PCI-listed P2PE solution, a PCI-listed MPOS EMV acceptance solution, or EMV payment tokenization may participate in VEP.

How can qualifying merchants apply for VEP?

Merchants that meet the qualification criteria for VEP should 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.

Does an acquirer have to report merchants participating in VEP to Mastercard?

Yes. A qualifying Level 1 or 2 merchant participating in VEP must be reported on the semiannual SDP Acquirer Submission and Compliance Status Form (SDP Form).

Does a merchant participating in VEP have to maintain compliance with the PCI DSS?

Yes. A merchant participating in VEP must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement. A merchant should check with their acquirer who may still require PCI DSS compliance validation from their merchant or may accept other forms of evidence of compliance which certifies eligibility for VEP.

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 VEP?

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 VEP.

What if a merchant does not satisfy VEP's eligibility criteria?

A merchant that does not satisfy VEP's eligibility criteria must continue to either validate its PCI DSS compliance annually in accordance with section 2.2.2 Merchant Compliance Requirements of the *Security Rules and Procedures*, or if eligible, may choose an alternative method for validating compliance with the PCI DSS (refer to section 2.2.4 Mastercard Cybersecurity Incentive Program [CSIP] of the *Security Rules and Procedures*).

Is VEP applicable to Level 1 and 2 service providers under the Mastercard SDP Program?

No. VEP is only applicable to merchants.

For More Information

For more information on the Validation Exemption Program, contact the SDP Team at 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