MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Compliance and Validation Exemption Program

APRIL 2025

Background
Mastercard offers merchants using secure technologies such as EMV technology, a Payment Card Industry Security Standards Council (PCI SSC)-listed point-to-point encryption (P2PE) solution, or a mobile point-of-sale (MPOS) EMV acceptance solution 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).

A merchant's participation in the CSIP is optional and can either reduce a merchant's PCI DSS compliance validation requirements through the Risk-based Approach or eliminate the requirement to annually validate PCI DSS compliance to Mastercard through the Validation Exemption Program (VEP).

Compliance and Validation Exemption Program
In March 2025, Mastercard announced the introduction of a new, optional program under the Mastercard CSIP called the Compliance and Validation Exemption Program (C-VEP), which exempts eligible merchants from the requirement to comply with the PCI DSS and annually validate their compliance with the PCI DSS to Mastercard.

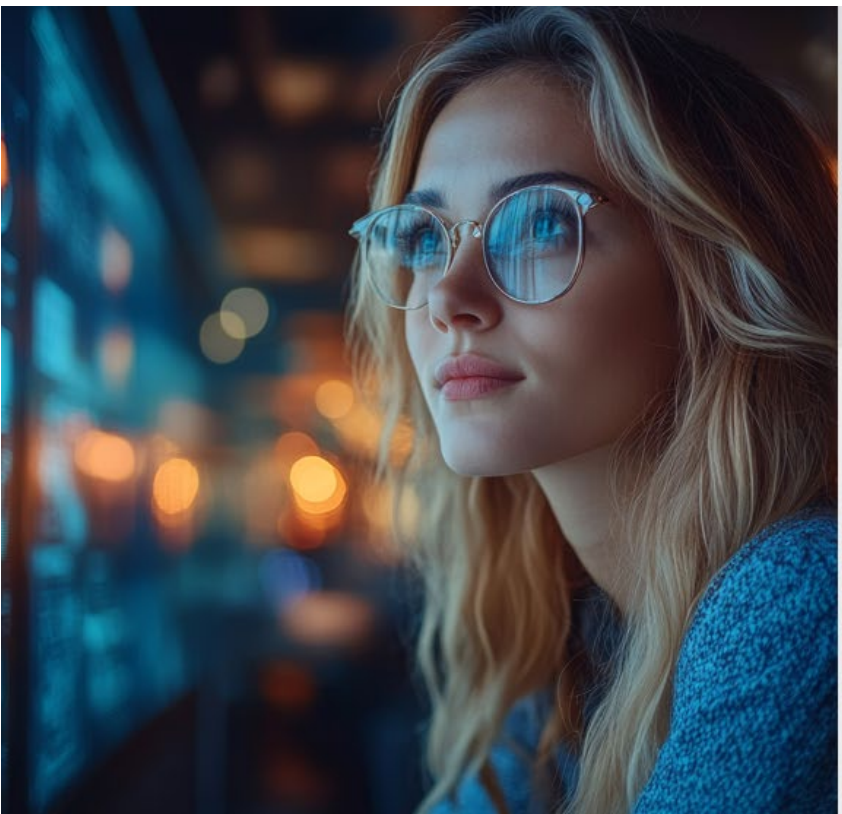
C-VEP EXEMPTS A MERCHANT FROM COMPLYING WITH THE PCI DSS & VALIDATING COMPLIANCE TO MASTERCARD

This program is available to Level 3 merchants (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) and Level 4 merchants (merchants with one million or fewer card-present transactions and 20,000 or fewer e-commerce transactions annually) that integrate a defined, comprehensive suite of cybersecurity and risk management tools into their environment through their acquirer.

Eligibility Requirements
To qualify for C-VEP, a Level 3 or 4 merchant, and their acquirer 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.
- ✓ The acquirer provides a suite of cybersecurity and risk management tools to the merchant as defined in the *Security Rules and Procedures*—2.2.4 Mastercard Cybersecurity Incentive Program (CSIP).

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



AT A MINIMUM

- Ongoing risk assessment and scoring
- Web malware monitoring
- ID theft protection
  - Dark web monitoring
  - Online social media monitoring
  - Credit monitoring
  - Human-based ID theft remediation service
- Security awareness education

REMEDIATION TOOLS

- Endpoint protection
  - Anti-virus
  - File integrity monitoring
  - Policy scanning
  - Endpoint threat detection
- Website script inventory and monitoring
- Authenticated vulnerability management
- Network threat detection and protection
  - Domain name system (DNS) security
  - BOT protection
  - Web application firewall
- Security information and event management (SIEM)
- Data encryption management

Frequently Asked Questions

The following list of questions is designed to assist Level 3 and 4 merchants who integrate a comprehensive suite of cybersecurity and risk management tools into their environment through their acquirer with SDP Program Standards for the Compliance and Validation Exemption Program.

What is C-VEP?

C-VEP is a new optional global program under the Mastercard CSIP, a component of the SDP Program, that allows qualifying merchants to be exempt from complying with the PCI DSS and annually validating their compliance with the PCI DSS to Mastercard.

Which merchants are eligible to participate in C-VEP?

A qualifying Level 3 or 4 merchant that integrates a defined, comprehensive suite of cybersecurity and risk management tools into their environment through their acquirer may participate in C-VEP, unless a merchant's participation conflicts with applicable law or regulation requiring such compliance and validation.

Is C-VEP applicable to Level 1 and 2 merchants under the Mastercard SDP Program?

No. C-VEP is only applicable to Level 3 and 4 merchants under the Mastercard SDP Program.

How can qualifying merchants participate in C-VEP?

To participate in C-VEP, a merchant and their acquirer must satisfy all the requirements as defined in section 2.2.4 Mastercard Cybersecurity Incentive Program (CSIP) of the *Security Rules and Procedures*.

Does participation in C-VEP exempt a merchant from complying with the PCI DSS and annually validating their compliance to Mastercard?

Yes. A merchant participating in C-VEP is no longer required to comply with the PCI DSS and annually validate their compliance to Mastercard.

Who should a merchant contact for more information on C-VEP?

Merchants should contact their acquiring bank for more information on C-VEP. It is the responsibility of the merchant's acquirer to validate that the merchant meets all the program requirements.

How can a merchant obtain a suite of cybersecurity and risk management tools as defined under C-VEP?

A merchant can obtain a suite of cybersecurity and risk management tools only through their acquirer.

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 C-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 C-VEP.

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

A merchant that does not satisfy C-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*).

For More Information

For more information on the Compliance and 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