MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Revised PCI DSS Compliance Requirements for L2 Merchants

MARCH 2021

mastercard

Background

Since June 2011, Mastercard has required Level 2 merchants (merchants with more than one million but less than or equal to six million transactions annually) to complete their annual Payment Card Industry Data Security Standard (PCI DSS) compliance validation using a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA) approved by the PCI Security Standards Council (SSC). To validate compliance, a Level 2 merchant could either undergo an annual PCI DSS assessment resulting in the completion of a Report on Compliance (ROC) or a complete a Self-Assessment Questionnaire (SAQ) to meet Mastercard Site Data Protection (SDP) Program requirements.

Level 2 merchants that chose to validate their annual compliance validation by successfully completing an SAQ, a self-validation tool to assess security for cardholder data, and the associated Attestation of Compliance (AOC), a certification that a merchant is eligible to perform and have performed the appropriate SAQ, were still required to have a QSA or ISA to conduct the self-assessment. This Mastercard SDP Program requirement included merchants completing any one of the eight SAQ types based on how they accept payment cards.

Mastercard Update

The SDP Program is designed as a risk-based approach towards merchant PCI DSS compliance. Merchant levels are classified by payment channels and annual Mastercard and Maestro transaction volume. As previous compliance requirements for Level 2 merchants took a one-size fits all approach, low security risk card-present merchants using specific payment acceptance methods such as imprint machines or standalone, dial-out terminals with no electronic cardholder data storage were also required to engage a QSA or ISA to complete their annual compliance validation requirements.

To better reflect the cybersecurity risks of today and provide acquirers and their Level 2 merchants with a more uniformed industry approach, Mastercard has revised Level 2 merchant compliance validation requirements by eliminating the requirement to undergo an annual PCI DSS assessment and the associated completion of a ROC, and instead only require that Level 2 merchants validate their compliance annually using an SAQ.

Effective March 2021, Level 2 merchants completing SAQ A, A-EP or D will still be required to engage a QSA or ISA for compliance validation as these are considered high security risk merchants (complex payment acceptance environments and/or ecommerce merchants). However, low security risk Level 2 merchants completing SAQ B, B-IP, C-VT, C or P2PE may now self-assess without the use of a QSA or ISA for compliance validation.

Note—Level 2 merchants, at their own discretion, may engage a QSA or ISA to complete a ROC instead of performing an SAQ.

OLD Rule

Level 2 Merchant Compliance Requirements

To validate compliance, a Level 2 merchant could either undergo an annual PCI DSS assessment resulting in the completion of a ROC **OR** complete an annual SAQ.

Level 2 merchants completing SAQ A, A-EP, B, B-IP, C-VT, C, P2PE or D were required to engage a QSA or ISA for compliance validation.

NEW Rule

Level 2 Merchant Compliance Requirements

To validate compliance, a Level 2 merchant is required to complete an annual SAQ[1].

Level 2 merchants completing SAQ A, A-EP or D are required to engage a QSA or ISA for annual compliance validation. Level 2 merchants completing SAQ B, B-IP, C-VT, C or P2PE may now self-assess without the use of a QSA or ISA for compliance validation.

[1] Effective March 2021

PCI DSS SAQ Types

There are eight PCI DSS SAQs available on the PCI SSC website to meet different merchant environments. Each document was developed to help merchants determine which SAQ best applies to their environment. Level 2 merchants are recommended to work with their acquirers on determining the appropriate SAQ for their payment environment.

- *SAQ A*—Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced
- *SAQ A-EP*—Partially Outsourced E-Commerce Merchants Using a Third-Party Website for Payment Processing
- *SAQ B*—Merchants with Only Imprint Machines or Only Standalone, Dial-Out Terminals
- *SAQ B-IP*—Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals
- *SAQ C-VT*—Merchants with Web-Based Virtual Terminals
- *SAQ C*—Merchants with Payment Application Systems Connected to the Internet
- *SAQ P2PE*—Merchants using Only Hardware Payment Terminals in a PCI SSC-listed P2PE Solution
- *SAQ D*—All Other SAQ-Eligible Merchants

Frequently Asked Questions

The following list of questions is designed to assist acquirers and their merchants on revised Level 2 merchant PCI DSS compliance validation requirements.

What are the new PCI DSS compliance validation requirements for Level 2 merchants?
Level 2 merchants (merchants with more than one million but less than or equal to six million transactions annually) are required to only complete an annual SAQ. However, Level 2 merchants completing SAQ A, A-EP or D must additionally engage a QSA or ISA for annual compliance validation. Level 2 merchants completing SAQ B, B-IP, C-VT, C or P2PE may now self-assess without the use of a QSA or ISA for compliance validation.

Why has Mastercard revised Level 2 merchant PCI DSS compliance requirements?
Mastercard has revised Level 2 merchant PCI DSS compliance requirements to better reflect the cybersecurity risks of today and provide acquirers and their merchants with a

more uniformed industry approach for lower security risk merchants (for example, merchants using imprint machines or standalone, dial-out terminals with no electronic cardholder data storage).

Can Level 2 merchants continue to engage a QSA or ISA to complete a ROC instead of performing an SAQ?
Yes. Level 2 merchants, at their own discretion, may continue to engage a QSA or ISA to complete a ROC instead of performing an SAQ.

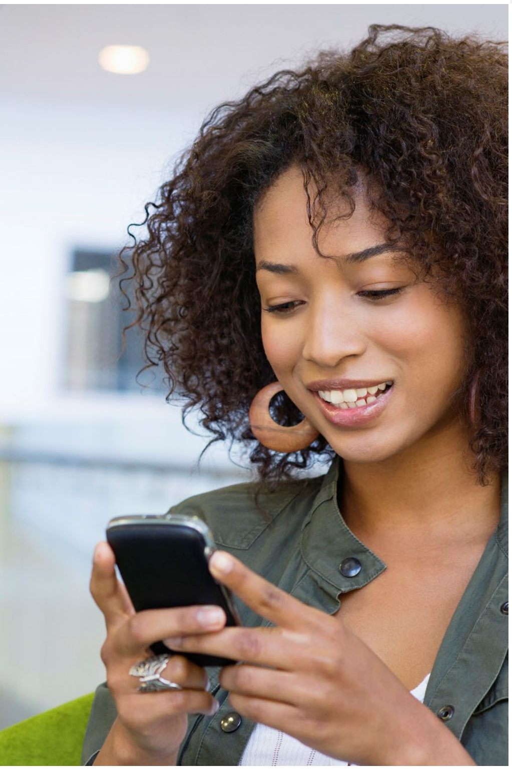
Are Level 2 merchants still required to undergo an annual PCI DSS assessment resulting in the completion of a ROC?
No. Mastercard has eliminated the requirement to undergo an annual PCI DSS assessment resulting in the completion of a ROC. Level 2 merchants are now required to validate PCI DSS compliance annually using an SAQ.

If a Level 2 merchant is completing a SAQ A, A-EP or D, will they still be required to engage a QSA or ISA for annual compliance validation?
Yes. Level 2 merchants completing SAQ A, A-EP or D will still be required to engage a QSA or ISA for compliance validation as these are considered high security risk merchants (complex payment acceptance environments and/or ecommerce merchants).

If a Level 2 merchant is completing SAQ B, B-IP, C-VT, C or P2PE, will they still be required to engage a QSA or ISA for annual compliance validation?
No. Level 2 merchants completing SAQ B, B-IP, C-VT, C or P2PE may now self-assess without the use of a QSA or ISA for compliance validation.

Do the revised PCI DSS compliance validation requirements affect Level 1 merchants (merchants having more than six million transactions annually)?
No. The revised PCI DSS compliance validation requirements do not apply to Level 1 merchants. Level 1 merchants are required to undergo an annual PCI DSS assessment resulting in the completion of a ROC conducted by a QSA or ISA.

Where can Level 2 merchants find the PCI DSS Self-Assessment Questionnaires?
PCI standards documentation, reporting templates and forms including the PCI DSS Self-Assessment Questionnaires can be found on the PCI SSC website at www.pcisecuritystandards.org/document_library.



For More Information

For more information on revised Level 2 merchant PCI DSS compliance validation requirements, please send an email to the SDP Program mailbox: sdp@mastercard.com. In addition, the following resources are available to you:

Mastercard

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

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

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

©2021 Mastercard. Proprietary. All rights reserved.