MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

PCI Data Security Essentials Resources for Small Merchants

OCTOBER 2018

mastercard

www.mastercard.com/sdp

PCI DSS COMPLIANCE IS REQUIRED FOR L4 MERCHANTS

Although an acquirer is not required to report the PCI compliance status of their L4 merchants to Mastercard, a L4 merchant is still required to be PCI compliant as per SDP Standards.

To validate PCI DSS compliance, a L4 merchant must successfully complete:

- **an annual SAQ; and**
- **quarterly network scans conducted by a PCI ASV.**

Alternatively, a L4 merchant may engage a PCI QSA for an onsite assessment.

For more information on acquirer compliance requirements or L4 merchant validation requirements, you can review 10.3.3 and 10.3.4 of the Security Rules and Procedures Manual.

Background

In the Global Operations Bulletin No. 3, 1 March 2017, Mastercard announced that effective 31 March 2019, an acquirer must certify that it has a risk management program in place to identify and manage security risk within their Level 4 merchant portfolio. It is important for acquirers that have not yet implemented a Level 4 merchant risk management program to begin the process as soon as possible to meet this Site Data Protection (SDP) Program requirement's deadline. We recommend reviewing Mastercard's Guidance for Level 4 Merchant Risk Management Program document which is intended to provide requirements and recommendations for implementing a Level 4 risk management program acceptable to Mastercard.

Mastercard Update

SDP Program Standards require that Level 4 merchants comply with the Payment Card Industry (PCI) Data Security Standard (DSS) and may validate compliance by completing an annual Self-Assessment Questionnaire (SAQ) and quarterly network scans conducted by a PCI Security Standards Council (SSC) Approved Scanning Vendor (ASV). A Level 4 merchant may alternatively engage a PCI SSC approved Qualified Security Assessor (QSA) for an onsite assessment instead of performing a self-assessment.

With the recent launch of the PCI SSC's updated PCI Data Security Essentials Resources for Small Merchants and a new Data Security Essentials Evaluation Tool aimed at helping small business owners protect their customer's payment card data, Mastercard is recommending that Level 4 merchants use these educational resources as additional guidance tools while working towards achieving PCI DSS compliance.

PCI Data Security Essentials

PCI Data Security Essentials for Small Merchants provide easy-to-use information as a starting point for small businesses to understand how to protect themselves and their customers and have been updated to address the current and evolving threats small merchants face today. The Data Security Essentials evaluations offer an alternative way small merchants can evaluate and report how they are meeting security basics for safe payments while demonstrating progress towards PCI DSS compliance.

The Data Security Essentials online tool and evaluation form conducts a preliminary evaluation of a small merchant's most common, critical risks of their payment environment to see where they stand with payment security practices. We encourage acquirers to download these resources and start educating their small business customers on payment security basics:

Guide to Safe Payments
Simple guidance for understanding the risk to small businesses, security basics to protect against payment data theft, and where to go for help.

Common Payment Systems
Real-life visuals to help identify what type of payment system small businesses use, the kinds of risks associated with their system, and actions they can take to protect it.

Questions to Ask Your Vendors
A list of the common vendors small businesses rely on and specific questions to ask them to make sure they are protecting customer payment data.

Glossary of Payment and Information Security Terms
Easy-to-understand explanations of technical terms used in payment security.

www.pcisecuritystandards.org

The Data Security Essentials Evaluation Tool is an easy-to-use guide aimed at helping small merchants focus on essential payment data security practices needed to protect payment data and reduce risk in their business environment.

The online tool provides a way for merchants to conduct a preliminary evaluation of their security posture.

PCI Firewall Basics
A one-page infographic on firewall configuration basics.

Data Security Essentials Evaluation Tool
An online tool with accompanying evaluation forms which provides a way for merchants to conduct a preliminary evaluation of their security posture.

Frequently Asked Questions

The following list of questions is designed to assist acquirers and their Level 4 merchants on how Mastercard has incorporated the use of PCI Data Security Essentials Resources into SDP Program Standards.

Is Mastercard requiring Level 4 merchants to use the PCI Data Security Essentials Evaluation Tool?
No. Mastercard is only recommending that Level 4 merchants use the Data Security Essentials Evaluation Tool as an additional guidance tool while working towards achieving PCI DSS compliance.

Should an acquirer include the Data Security Essentials Evaluation Tool/resources into their Level 4 risk management program?
Yes. The PCI Data Security Essentials Tool and resources for small merchants provide security basics to protect against payment data theft and to help small merchants simplify their security and reduce their risk.

Once a Level 4 merchant completes the Data Security Essentials Evaluation Tool and associated evaluation form, are they considered PCI DSS compliant?
No. A Level 4 merchant that completes the Data Security Essentials Evaluation Tool and associated evaluation form is not considered PCI DSS compliant. To validate PCI DSS compliance, a Level 4 merchant must successfully complete an annual SAQ and quarterly network scans conducted by a PCI ASV; or they may alternatively engage a PCI QSA for an onsite assessment.

Besides using Data Security Essentials Resources, what other resources can an acquirer use as guidance to assess the risk of their Level 4 merchant portfolio?
In addition to using the PCI Data Security Essentials Resources when assessing the risk of an acquirer's Level 4 merchant portfolio, we encourage acquirers to review Mastercard's Guidance for Level 4 Merchant Risk Management Program document which is intended to provide requirements and recommendations for implementing a Level 4 risk management program acceptable to Mastercard.

For More Information

For more information on PCI Data Security Essentials Resources for Small Merchants, 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 complimentary 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.

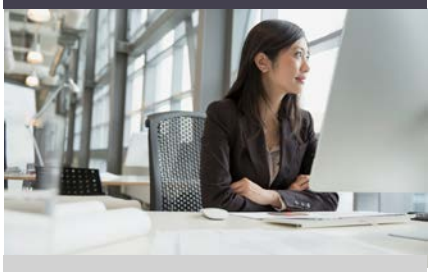
Mastercard PCI 360 Education Portal: www.mastercard.com/pci360
Mastercard Site Data Protection Program Site: www.mastercard.com/sdp

The Payment Card Industry Security Standards Council

The PCI SSC provides a wide array of documentation on its website as well as a "micro-site" dedicated to small merchants.

PCI Security Standards Council Site: www.pcisecuritystandards.org
PCI Data Security Essentials Resources for Small Merchants Site: www.pcisecuritystandards.org/merchants/

www.mastercard.com/pci360



For additional frequently asked questions about the Mastercard SDP Program, such as compliance validation requirements for L1-4 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.