MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Guidance for Level 4 Merchant Risk Management Program

JULY 2018

mastercard

ACQUIRER CERTIFICATION OF L4 MERCHANT RISK MANAGEMENT PROGRAM

Background

Mastercard Site Data Protection (SDP) Program rules require all entities that store, transmit, or process cardholder data, regardless of size, to comply with all Payment Card Industry Data Security Standard (PCI DSS) requirements. Merchants with one million or fewer card-present transactions and 20,000 or fewer e-commerce transactions are defined by Mastercard as Level 4 merchants. Although an acquirer is not required to validate the PCI DSS compliance status of its Level 4 merchants to Mastercard, a Level 4 merchant is still required to be PCI DSS compliant and may validate compliance by successfully completing an annual Self-Assessment Questionnaire (SAQ) and quarterly network scans conducted by a Payment Card Industry Security Standards Council (PCI SSC) Approved Scanning Vendor (ASV). A Level 4 merchant may alternatively, at their own discretion, engage a PCI SSC approved Qualified Security Assessor (QSA) for an onsite assessment.

Update

In the Global Operations Bulletin No. 3, 1 March 2017, Mastercard announced revisions to the SDP Program Standards. Revisions to the Program include an acquirer certification of a Level 4 merchant risk management program. Effective 31 March 2019, an acquirer must certify to Mastercard that it has a risk management program in place to identify and manage security risk within the acquirer's Level 4 merchant portfolio.

An additional - yes or no - question has been added to the SDP Acquirer Submission and Compliance Status Form for acquirers to attest to having a risk management program in place for their Level 4 merchant portfolio. The new data field on the form will need to be completed by the acquirer beginning 31 March 2019.

If an acquirer has an existing risk management program that meets the requirements detailed below, the acquirer is not obligated to change the contents of their current program.

Guidance

This guidance document is intended to provide *requirements* and *recommendations* for an acquirer looking to implement a Level 4 risk management program by 31 March 2019 to meet SDP Program requirements. An acquirer's compliance program for Level 4 merchants must meet all requirements. If an acquirer has an existing risk management program that meets the requirements detailed below, the acquirer is not obligated to change the contents of their current program. The program may or may not include the below recommendations. Each acquirer is responsible for determining the most effective methods to manage their risk for their Level 4 merchants.

Requirements

When implementing a Level 4 merchant risk management program, an acquirer must include the following elements:

- ✓ *Know who your Level 4 merchants are.* A merchant that is not deemed to be a SDP L1, L2, or L3 merchant is a L4 merchant.
- ✓ *Rank your Level 4 merchants based on risk.*
  - Categorize merchants by industry verticals (hospitality, retail, grocery, etc.)
  - Understand how merchants accept payments (dial-up terminals, IP connected terminals, networked terminals, fully outsourced, e-commerce, etc.)
  - Identify high-risk merchants (for example, merchants with large networks of connected POS systems processing payments) vs. low-risk merchants (for example, merchants with a single dial-up terminal)
  - Identify use of third parties such as terminal servicers that may impact the underlying security of your merchants
- ✓ *Regularly communicate PCI DSS compliance requirements to high-risk Level 4 merchants*. This formal communication could be through the use of emails, letters, mailers, newsletters, contracts, account statements, etc.
- ✓ *Manage and set deadlines for your high-risk Level 4 merchants to submit PCI DSS validation documents.* An effective alternative to full PCI DSS validation may include utilizing the PCI DSS Prioritized Approach which provides a framework for compliance efforts using six security milestones to help identify the highest risk targets within an organization.
- ✓ *Validate your high-risk Level 4 merchants' compliance with the PCI DSS.* Review merchant submissions of SAQs, network scan reports, and Reports on Compliance (ROC), if applicable, to determine that a merchant is in compliance with the PCI DSS. It is the acquirer's responsibility to monitor a merchant's compliance and ensure that merchants are protecting cardholder data in accordance with the PCI DSS.

The PCI SSC's Payment Protection Resources for Small Merchants may be helpful with the identification of merchant acceptance channels.

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

Recommendations

When implementing a Level 4 merchant risk management program, an acquirer should consider the following elements:

- ✓ *Encourage your Level 4 merchants to use payment technologies that devalue and desensitize payment card data.* Secure payment technologies include EMV, validated Point-to-Point Encryption (P2PE) Solutions listed on the PCI SSC's website, and Tokenization products.
- ✓ *Encourage your Level 4 merchants to utilize the latest approved PCI PIN Transaction Security (PTS) devices (currently version 5.x).* Merchants implementing new payment devices must use only PCI PTS-approved devices in their payment environments.
- ✓ *Ensure that your Level 4 merchants use only PCI DSS compliant Service Providers.* The Mastercard SDP Compliant Registered Service Provider List is updated monthly and only lists Service Providers that have been registered with Mastercard and have successfully completed an onsite assessment conducted by a PCI SSC approved QSA.
- ✓ *Validate that your Level 4 merchants use payment applications that are compliant with the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS), as applicable.* Payment applications that are eligible for PCI PA-DSS validation are defined in the PCI PA-DSS Program Guide.
- ✓ *Recommend that your Level 4 merchants use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website when implementing or supporting a payment application compliant with the PCI PA-DSS.*
- ✓ *Encourage your high-risk Level 4 merchants to engage a PCI SSC approved QSA or use a PCI Internal Security Assessor (ISA) when assessing their PCI DSS compliance.*
- ✓ *Provide awareness to your Level 4 merchants on the most common points of compromise occurring in small merchant networks including but not limited to:*
  - **Insecure remote access**, which amounts to the initial point of entry of nearly 80% of all Level 4 merchant compromises. Ensure your Level 4 merchants adhere to PCI DSS requirements on properly securing remote access.
  - **Insecure third party Service Providers**, for example, POS vendors and terminal servicers, which account for a significant percentage of Level 4 merchant account data compromises. Even if a Service Provider does not store, does not process, and does not transmit cardholder data, but is connected-to or has access to cardholder data (whether intended or not), that Service Provider could impact the security of cardholder data and must be validated compliant with all applicable PCI DSS requirements.

The goal of your L4 merchant risk management program is to identify and manage security risk within your L4 portfolio as well as help protect merchants from account data compromises.

Do your L4 merchants use only:

- *Secure payment technologies (EMV, P2PE, Tokenization)*
- *Approved PCI PTS devices*
- *PCI DSS compliant Service Providers*
- *QIRs to implement PCI PA-DSS payment applications*
- *Secure remote access*

For More Information

For more information on an acquirer's Level 4 merchant risk management 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 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 Payment Protection Resources for Small Merchants Site: www.pcisecuritystandards.org/merchants/