MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

Guidance for Terminal Servicer PCI DSS Validation

AUGUST 2017

Purpose

This document is intended to provide guidance to Terminal Servicers on which Payment Card Industry Data Security Standard (PCI DSS) requirements may likely apply to their PCI DSS validation.

Introduction

A Terminal Servicer is an entity that provides ongoing maintenance and support of a payment terminal. Terminal Servicers generally do not store, process, or transmit Cardholder Data but are "connected-to" the merchant Cardholder Data Environment (CDE).

Terminal Servicers equip merchants with technologies that allow Mastercard cardholders to pay with a variety of methods including magnetic stripe plastic cards, contactless, EMV chip-enabled cards, and a variety of mobile wallet applications. Terminal Servicers may also provide services that assist merchants with the administration of the point-of-sale (POS) systems and maintain compliance with PCI Standards.

A Terminal Servicer can support hundreds to thousands of merchants through remote access links or other back door access methods to the merchants' systems. Such methods of remote access are widely used by small and large businesses, but are often installed or configured incorrectly, resulting in the insecure implementation of remote access software. Terminal Servicers that are not PCI DSS compliant have led to account data compromise (ADC) events.

TERMINAL SERVICERS ARE REQUIRED TO BE REGISTERED WITH MASTERCARD AND MUST VALIDATE PCI DSS COMPLIANCE

In the *Global Operations Bulletin* No. 7, 3 July 2017, Mastercard introduced a new Service Provider type – Terminal Servicer (TS).

All Terminal Servicers must be registered with Mastercard.

Mastercard Site Data Protection (SDP) Program

In *Global Operations Bulletin* No. 8, 1 August 2017, Mastercard announced the addition of Terminal Servicers as Level 2 Service Providers under the Site Data Protection (SDP) Program Standards (Chapter 10, Section 3, of the Mastercard Security Rules & Procedures). All Level 2 Service Providers are required to validate their PCI DSS compliance to Mastercard annually via a PCI DSS Self-Assessment Questionnaire (SAQ) as provided on the PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org). The applicable SAQ for a Terminal Servicer is PCI SAQ D for Service Providers (PCI SAQ D-SP).

PCI SAQ D for Service Providers (PCI SAQ D-SP)

The PCI SSC has designed an SAQ for Service Providers who self-assess their PCI DSS compliance validation, which means the Service Provider does not utilize the services of a Qualified Security Assessor (QSA). PCI SAQ D-SP includes hundreds of requirements, mapped to the PCI DSS, many of which may not apply to Terminal Servicers.

Since Terminal Servicers generally do not store, process, or transmit Cardholder Data, there are a limited set of PCI DSS requirements that are applicable to Terminal Servicers. This guidance document provides a suggested set of PCI DSS requirements that may apply to a Terminal Servicer. However, it is important to note this is not intended to cover every implementation or every Terminal Servicer as each entity may implement people, process, and technology differently. As such, it's important for each individual Terminal Servicer to properly scope their PCI DSS environment appropriately (guidance on scoping is available on the PCI SSC website).

Once registered with the Mastercard Service Provider Registration Team, the PCI SAQ D-SP Attestation of Compliance (AOC) should be sent to the SDP Team.

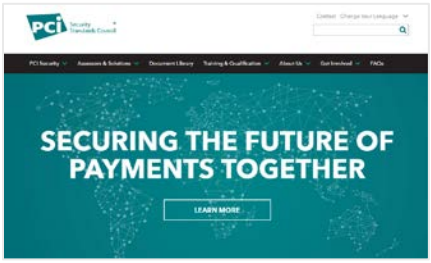
Although not required, Mastercard recommends, as a best practice, Terminal Servicers engage a QSA and perform a full on-site assessment with a Report on Compliance (ROC) to annually validate PCI DSS compliance instead of completing a PCI SAQ D-SP.

Guidance for Suggested Requirements

The following list of PCI DSS requirements is intended to provide guidance for Terminal Servicers who generally do not store, process, or transmit Account Data but rather are only "connected-to" a merchant's CDE. The listed requirements are not meant to replace the guidance and expertise of a QSA, nor to be an authorative and exhaustive list of all PCI DSS requirements that should be implemented by a Terminal Servicer. This guidance document is intended to communicate a suggested minimum set of PCI DSS requirements to which a Terminal Servicer must validate compliance.

The table below highlights 90 of the 256 total requirements in the PCI SAQ D-SP, a subset of requirements that comprise the full SAQ.

PCI DSS Req. #	Requirements Applicable
Requirement 1	None
Requirement 2	2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3, 2.4, 2.5
Requirement 3	None
Requirement 4	None
Requirement 5	All
Requirement 6	6.1, 6.2, 6.3, 6.3.1, 6.6, 6.7
Requirement 7	All
Requirement 8	All
Requirement 9	None
Requirement 10	10.1, 10.2.x, 10.3.x, 10.7
Requirement 11	None
Requirement 12	12.1, 12.1.1, 12.4, 12.5, 12.6, 12.8.x, 12.9, 12.10.x



PCI DSS Requirements, *Testing Procedures*, and *Guidance* for validating compliance can be found in the PCI DSS, available for free to the public, and located on the PCI Council's website: www.pcisecuritystandards.org.

For More Information
For more information on PCI DSS validation for Terminal Servicers, 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 including tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.

PCI Security Standards Council Site: www.pcisecuritystandards.org
PCI Document Library: www.pcisecuritystandards.org/document_library

Disclaimer
Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties. This guidance does not constitute an endorsement or warranty by Mastercard regarding the security of any Terminal Servicer.