MASTERCARD SECURITY RULES & PROCEDURES

New Cybersecurity Standards & Programs Chapter

OCTOBER 2019

mastercard

CUSTOMER COMPLIANCE WITH THE NIST CYBERSECURITY FRAMEWORK

Overview

Mastercard is introducing a new "Cybersecurity Standards and Programs" chapter to the *Security Rules and Procedures (SR&P)* manual. The new chapter provides an overview of relevant cybersecurity standards, including those published by the Payment Card Industry (PCI) Security Standards Council (SSC). It describes mandates and best practice recommendations for customers and their agents to ensure baseline cybersecurity controls are implemented and maintained.

The key objectives of the Cybersecurity Standards and Programs chapter were to establish new cybersecurity best practices for securing a customer's non-Cardholder Data Environment (CDE) and bring together into a single chapter existing rules and compliance programs relating to the PCI Security Standards including the Mastercard Site Data Protection (SDP) Program, the Global Vendor Certification Program (GVCP) and Card Production Standards, and PIN Security Requirements.

What is New?

For environments where the PCI Data Security Standard (DSS) or another PCI standard does not apply, but where security assurance remains necessary, all customer environments, systems or devices used to store, process or transmit confidential information are recommended to comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) or one of the standards included as Informative References to the NIST CSF.

Customer environments that store, process, or transmit account data must continue to comply with the PCI DSS in accordance with existing Mastercard SDP Program Standards, and all other applicable PCI Standards and Programs as defined in the new Cybersecurity Standards and Programs chapter in the SR&P manual.

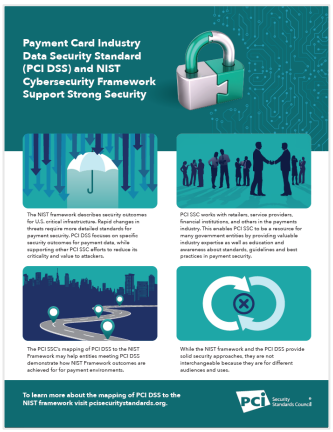
As a best practice, all customer environments, systems or devices used to store, process or transmit confidential information are recommended to comply with the NIST CSF and/or the requirements contained in the NIST CSF list of "Informative References" documents.

Customer environments that store, process, or transmit account data must continue to comply with the PCI DSS, in accordance with SDP Program Standards.

PCI DSS to NIST CSF Mapping

The PCI SSC has published three resources to assist entities working with both the PCI Data Security Standard and the NIST Cybersecurity Framework. These resources and supporting guidance documents include a mapping of PCI DSS v. 3.2.1 which provides specific security requirements for payment card data to the NIST CSF v. 1.1 which provides broad security and risk management objectives:

Mapping PCI DSS to NIST Cybersecurity Framework



Mapping PCI DSS to NIST Cybersecurity Framework - Executive Brief

Mapping PCI DSS to NIST Cybersecurity Framework At-a-Glance Summary

What has Changed?
In addition to introducing new Cybersecurity Standards for customer environments where PCI Security Standards do not apply, Mastercard has consolidated existing PCI compliance programs under a single chapter. This change was designed to organize current requirements for entities that are affected by any of the PCI Security Standards and provide clarity by updating rules to reflect new versions of the standards.

Previously, Mastercard organized PCI compliance programs as their own chapters in the SR&P manual, which caused customers, merchants, service providers and vendors to overlook their obligations and not fully understand which PCI requirements apply to them. Having the PCI standards and programs collected within a single Cybersecurity Standards and Programs chapter will enable all entities reviewing the new chapter to better determine which standard or standards apply to them. The following four areas are now covered within Chapter 2 of the SR&P manual:

Cybersecurity Standards
Minimum cybersecurity requirement for customer environments that store, process, or transmit account data and a best practice recommendation for securing a customer's non-CDE. Note—customer compliance validation to Mastercard is not required.

Site Data Protection Program
The SDP Program governs compliance obligations for all entities that store, process or transmit account data as well as validation obligations for merchants and registered service providers for the PCI Data Security Standard, PCI Payment Application Data Security Standard (PA-DSS), PCI Token Service Provider Standard (TSP), PCI 3DS Core Standard, and the PCI Qualified Integrator & Reseller Program (QIR). The SDP Program also maintains incentive programs and best practice recommendations for the PCI Point-to-Point Encryption Standard (P2PE), EMV Chip, PCI DSS Designated Entities Supplemental Validation (DESV), and 3DS SDK Standard.

Global Vendor Certification Program and Card Production Standards
The GVCP Program governs compliance and validation obligations for the PCI Card Production & Provisioning Security Requirements (Logical and Physical).

PIN Security Standards
PIN Security Standards mandates compliance with the PCI PIN Security Requirements, PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements, PCI PTS Hardware Security Module (HSM) Security Requirements and the PCI Software-based PIN Entry on COTS (SPoC) Security Requirements. Note—currently, there is no associated PIN security validation program.

Table of
CONTENTS—Cybersecurity Standards and Programs

Frequently Asked Questions

The following list of questions is designed to assist Mastercard customers with the NIST CSF compliance recommendation for environments where PCI Security Standards do not apply.

Why is Mastercard recommending that customers comply with the NIST CSF as a best practice for securing environments, systems or devices used to store, process or transmit confidential information?

Security of all customer environments where confidential information is stored, processed, or transmitted is vital to the safety and security of the global payments system. While the PCI standards have successfully helped secure CDEs around the world, their applicability and scope are limited to specific environments. For environments where the PCI standards do not apply, but where security assurance remains necessary, the NIST CSF and/or its Informative References will be recommended as a best practice.

Why is Mastercard recommending the NIST CSF over other security frameworks and standards?

The NIST CSF is complementary to the PCI DSS. They address common goals and principles for securing data. With the PCI SSC's recent publication of the detailed mapping between the PCI DSS and the NIST CSF, entities can successfully implement both.

Why is Mastercard recommending a US-centric standard?

The NIST CSF is a globally recognized cybersecurity standard with an overarching security and risk management structure. It incorporates detailed mappings to five (5) additional cybersecurity standards/frameworks, which offer a global footprint of cybersecurity standards providing Mastercard customers with flexibility and choice (refer to the PCI SSC's Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1 document).

Is Mastercard mandating that customers comply with the NIST CSF?

At this time, Mastercard is only recommending that customers use the NIST CSF or one of its Informative References as a best practice for securing all customer environments, systems or devices used to store, process or transmit confidential information.

Are customers required to validate compliance with the NIST CSF?

At this time, compliance with the NIST CSF is recommended as a best practice only. Validation of compliance to Mastercard is not required.

Are customers required to comply with the PCI DSS?

Yes. Customer environments that store, process, or transmit account data must comply with the PCI DSS, in accordance with the Mastercard SDP Program, and all other applicable PCI Security Standards.

Is Mastercard changing its PCI DSS mandate for customers (e.g. issuers, acquirers)?

No. Compliance with the PCI DSS is required for all issuers and acquirers, although validation of compliance to Mastercard is not required.

Is Mastercard replacing PCI DSS compliance with the NIST CSF compliance?

No. Compliance with the PCI DSS is required for customers to properly secure their CDE. The NIST CSF and/or its Informative References are recommended as a best practice for securing non-CDEs. The NIST CSF and the PCI DSS are complementary, but one does not replace the other.

The following list of questions is designed to assist card production vendors with PCI Card Production and Provisioning Standard compliance.

When is compliance with the PCI Card Production and Provisioning Security Requirements (PCI CP&P) enforced instead of or in addition to compliance with the PCI DSS?

Card production activities such as card manufacturing, personalization and provisioning must be performed in a high security area that is physically and logically separated from other activities an entity may perform. When card production activities are performed by a vendor, the card production environment is assessed for compliance with the PCI CP&P Standard. Entities that store, process, or transmit account data for activities other than card production must also comply with the PCI DSS.

What is the Global Vendor Certification Program (GVCP) and how can I obtain further information about this program?

The Global Vendor Certification Program assesses and enforces vendor compliance with the PCI CP&P Standard. The policies and procedures by which GVCP manages vendor compliance is documented in the *Card Vendor Certification Standards* manual available on Mastercard Connect under the "Publications" application. For questions about the Global Vendor Certification Program, contact GVCP-HelpDesk@mastercard.com.

For More Information
For more information on the new Cybersecurity Standards & Programs chapter in the SR&P manual, please send an email to the SDP Program mailbox: sdp@mastercard.com.

In addition, the following resources are available to you:

Mastercard
The Mastercard Site Data Protection 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 contains information including white papers and webinars on cardholder data security. This site offers beginner to expert level training curricula suitable for entities of all sizes and complexity.

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

National Institute of Standards and Technology
The National Institute of Standards and Technology is a non-regulatory agency of the United States Department of Commerce that promotes the NIST Cybersecurity Framework and a list of "Informative References" that map NIST requirements to other recognized cybersecurity standards.

NIST Cybersecurity Framework and NIST CSF Informative References:
https://www.nist.gov/cyberframework

AVAILABLE RESOURCES:

SDP Program
mastercard.com/sdp

PCI 360
mastercard.com/pci360

PCI Council
pcisecuritystandards.org

NIST
nist.gov/cyberframework