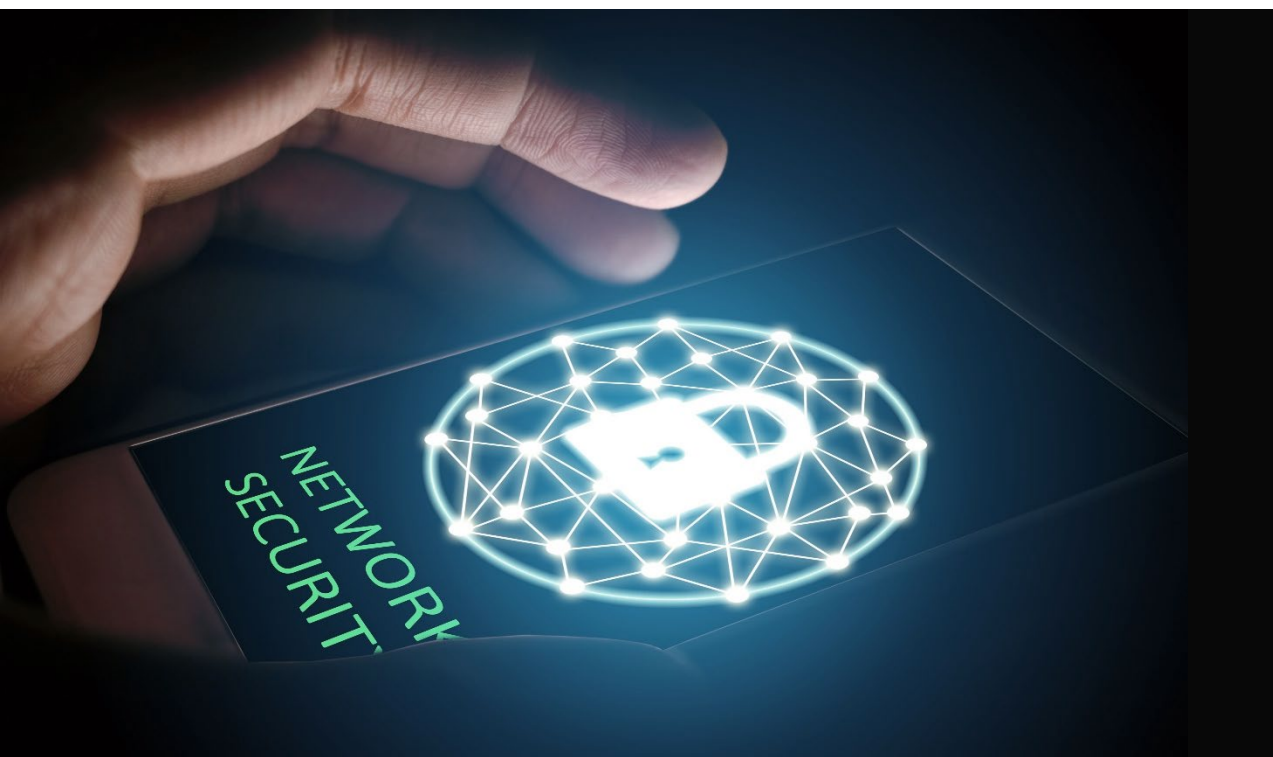


Q4 2019 PCI QUARTERLY NEWSLETTER



—Wishing You Happy Holidays from the Mastercard SDP Team—

MASTERCARD

NEWS & REMINDERS

Cybersecurity Best Practice for Customers

Last month, Mastercard introduced new Cybersecurity Standards for securing a customer's non-Cardholder Data Environment (CDE). To ensure baseline cybersecurity controls are implemented and maintained, Mastercard is recommending that all customer environments, systems, or devices used to store, process, or transmit confidential information comply with the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework \(CSF\)](#) and/or the requirements contained in one of its informative References.

For more information on this best practice recommendation, read *AN 3375—Revised Standards—New Cybersecurity Standards and Programs Chapter* available on [Mastercard Connect™](#).

PCI Standards and Programs—Rules Chapter

In addition to introducing a best practice recommendation for customers to establish meaningful cybersecurity controls, a new chapter has been added to the *Security Rules and Procedures* to consolidate existing PCI compliance programs under a single chapter. The "Cybersecurity Standards and Programs" chapter now includes information

IN THIS ISSUE

MASTERCARD

NEWS & REMINDERS

- Cybersecurity Best Practice for Customers
- PCI Standards and Programs - Rules Chapter
- SDP Form due 31 March 2020
- PTS POI V3.x Device Expiry Date
- AML/Sanctions Service Provider

RESOURCES / PCI 360

- Advancing New Cybersecurity Standards
- New Cybersecurity Standards & Programs Chapter
- PCI DSS Validation Exemption Program for Merchants Using Secure Technologies

EVENTS

- 2020 Cybersecurity & Risk Summit Series

PCI COUNCIL

NEWS & UPDATES

- PCI Contactless Standard
- P2PE V3.0
- PCI DSS V4.0 RFC Deadline
- Software Security Framework Assessor Program
- Card Production Security Assessor Program - Coming Soon

LATEST RESOURCES

- Key Blocks Blog Series
- Software Security Framework At-A-Glance
- Firewall Basics

EVENTS

- 2020 PCI SSC Events

TRAINING

- Acquirer Forum Webinar
- 2020 ISA ILT Schedule

on PCI Security Standards that were previously discussed in chapter 2 (relating to card production security), chapter 4 (relating to PIN security), and chapter 10 (relating to account data security/Mastercard SDP Program). Read [New Cybersecurity Standards & Programs Chapter](#).

SDP Form due 31 March 2020

The next [SDP Acquirer Submission and Compliance Status Form](#) (SDP Form) for Level 1, Level 2, and Level 3 merchant compliance reporting to Mastercard will be due on 31 March 2020. As a reminder, an acquirer must also certify to Mastercard via the SDP Form that it has a risk management program in place for their Level 4 merchants to identify and manage security risk. For more information on the next SDP Form submission deadline or questions on the [Level 4 risk management program certification](#), acquirers can send an email to sdp@mastercard.com.

PTS POI V3.x Device Expiry Date

PCI approval of devices validated against version 3.0 of the PTS POI Standard expires on 30 April 2020. The PCI Security Standards Council (SSC) will remove the expired V3 devices from the [PTS Approval list](#). This means that PTS POI V3 devices cannot be newly deployed in the Mastercard network after the expiry date. Devices already deployed may continue to operate until Mastercard announces a sunset date but should be replaced as soon as feasible with an approved version. For questions on PTS devices, send an email to POI_security@mastercard.com.

AML/Sanctions Service Provider

Effective 1 May 2020, Mastercard will establish a new Service Provider category—Anti-Money Laundering (AML)/Sanctions Service Provider—for third party entities that provide AML and Sanctions related services to customers. An AML/Sanctions

MASTERCARD

RESOURCES / PCI 360

[Advancing New Cybersecurity Standards](#)



Read how Mastercard has introduced Cybersecurity Standards as part of our rules to reflect and support the way we live and do business today.

By Adam Sommer—VP Industry Standards, Mastercard.

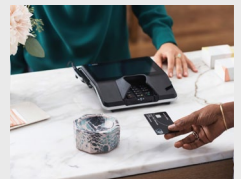
Download Mastercard's PCI [360](#) Educational Resources

[New Cybersecurity Standards & Programs Chapter](#)



This document discusses the new “Cybersecurity Standards and Programs” chapter in the *Security Rules and Procedures* and provides an overview of relevant cybersecurity standards, including PCI standards.

[PCI DSS Validation Exemption Program for Merchants Using Secure Technologies](#)



Learn how the Mastercard PCI DSS Validation Exemption Program eliminates the requirement to validate PCI compliance for card-present merchants using secure technologies.

KEY DATES—

31 MARCH 2020

30 APRIL 2020

1 MAY 2020

Service Provider will be classified as a [Level 1 Service Provider](#) under the SDP Program. After initial registration with [Mastercard](#), the AML/Sanctions Service Provider is required to contact the [SDP Team](#) and validate their compliance by submitting their PCI Data Security Standard (DSS) Attestation of Compliance (AOC).

EVENTS

2020 Cybersecurity & Risk Summit Series
The 2020 Mastercard Cybersecurity & Risk Summit Series by Global Risk Leadership (GRL) held in North America, Asia-Pacific, and Europe will take place on:

- North America: 1-4 June, Key Biscayne, Florida
- Asia-Pacific: 3-6 August, Bangkok, Thailand
- Europe: 5-8 October, Venice, Italy

Be sure to visit the [GRL website](#) to view conference and registration details for these

annual events happening next year. For more information on general questions, sponsorship information, or to inquire about speaking opportunities at our Global Risk Leadership events, send an email to globalrisk@mastercard.com.

PCI SECURITY STANDARDS COUNCIL NEWS & UPDATES

PCI Contactless Standard

The PCI SSC has now [published](#) the PCI Contactless Payments on COTS (CPoC™) Standard and Program Guide for solutions that enable merchants to accept contactless payments using a commercial off-the-shelf (COTS) mobile device (e.g., smartphone or tablet) with near-field communication (NFC). Using the [PCI CPoC Standard and supporting validation program](#), vendors can provide merchants with contactless acceptance solutions that have been developed and lab-tested to protect

MASTERCARD

EVENTS

Secure the Payments Ecosystem through Innovation and Collaboration

[2020 Cybersecurity & Risk Summit Series](#)



The GRL Conferences gather payments industry leaders from all around the world in the fraud and risk fields to collaborate on key safety and security issues impacting the industry.

PCI COUNCIL

LATEST RESOURCES

[Key Blocks Blog Series](#)



Read this blog series to learn more about how key blocks help secure payment data, its applicability, the 3 phases for implementing requirements and what AES and TDES block ciphers are.

[Software Security Framework At-A-Glance](#)



Download this new PCI SSC educational resource on the [PCI Software Security Framework](#) for an overview of what the SSF is, its benefits and how to use it.

CONTACTLESS
STANDARD—
NOW AVAILABLE

payment data. Read [Just Published: PCI Contactless Payments on COTS](#).

P2PE V3.0

The Point-to-Point Encryption (P2PE) V3.0 Standard and Program documents are expected to be published this month. The changes implemented for the latest version of the standard are a result of recommendations and feedback from industry stakeholders that will ultimately facilitate more P2PE Solutions to be available in the marketplace. P2PE V3.0 is focused on modernizing, simplifying, and adding flexibility to the Standard, Program, and assessment process. As a reminder, P2PE V2.0 Standard and Program will remain active for 18 months after V3.0 is published. Read [3 Things to Know About P2PE V3.0](#).

PCI DSS V4.0 RFC Deadline

The deadline to review and provide feedback on an early draft of PCI DSS V4.0 is approaching. The request for comments (RFC) period for the PCI DSS V4.0 will close on 13 December. All Participating Organizations, Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) are invited to participate. Specific timing on the next major release of the standard will be determined based on feedback received during the development period, but it is not anticipated for publication prior to late 2020. For more on the [RFC process](#), key priorities, and timing of the PCI DSS V4.0, read [3 Things to Know about PCI DSS V4.0 Development](#).

Software Security Framework Assessor Program

The PCI SSC has [launched](#) a new assessor qualification program to support the [PCI Software Security Framework \(SSF\)](#), a collection of standards and programs for the secure design, development, and maintenance of payment software. Through the SSF Assessor Program, PCI SSC qualifies

companies and their employees to assess vendors' software lifecycle management practices and payment software products to the [PCI Secure Lifecycle \(Secure SLC\) and Secure Software Standards](#). Read more on the [blog](#).

Card Production Security Assessor Program—Coming Soon

In January 2020, the PCI SSC will begin accepting applications for new (non-legacy) Card Production Security Assessors (CPSA). The [CPSA Program](#) will qualify companies and assessors to perform assessments using the [PCI Card Production Security Standards](#). The new CPSA Program will enhance consistency across assessments, provide guidance and ensure training is aligned with the current threat landscape. Training sessions will be available in June of 2020. Read [What to Know About the New Card Production Security Assessor Program](#).

EVENTS

2020 PCI SSC Events

The PCI SSC North America and Europe [Community Meetings](#) will take place in Orlando, Florida and Nice, France next year. Join the PCI Council and industry experts who will share the latest payment security updates and insights at the annual events. We encourage you to share the dates below with your customers and peers too so that they can begin planning ahead:

- 15-17 September: North America Community Meeting in Orlando, Florida, USA
- 20-22 October: Europe Community Meeting in Nice, France

Stay tuned for more on where the 2020 Asia-Pacific Community Meeting will be held.

PCI COUNCIL

LATEST RESOURCES *(continued)*

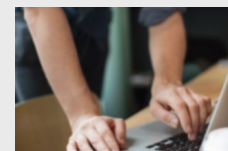
[PCI Firewall Basics](#)



A properly-configured firewall is vital to payment security. This one-page infographic provides guidance on security basics to help merchants properly configure firewalls.

TRAINING

[Acquirer Forum Webinar](#)



If you missed the Acquirer Forum webinar this month, it will be available to view on the PCI SSC's website shortly. Acquirers and processors are encouraged to listen to the webinar to get the latest updates on Council initiatives in 2020.

[2020 ISA ILT Schedule](#)



The 2020 PCI Internal Security Assessor (ISA) Instructor-Led Training (ILT) Schedule is now available. The two-day class improves understanding of PCI DSS and how it can help protect your customer payment data and business.