# Q2 2022 PCI Quarterly Newsletter

Service Provider Listing

## IN THIS ISSUE

MASTERCARD

UPDATES & REMINDERS

RESOURCES

EVENT

PCI COUNCIL

NEWS & UPDATES

SSC HIGHLIGHTS

EVENTS

TRAINING

Sign up to receive Mastercard's quarterly newsletter and the PCI Security Standards Council's (PCI SSC) PCI Perspectives blog. Additional PCI information and educational resources can also be found on Mastercard PCI 360 and pcisecuritystandards.org.

## Mastercard
## UPDATES & REMINDERS

*SDP Service Provider List & Expired Validation*

The Mastercard SDP Compliant Registered Service Provider List provides information about service providers that are registered with Mastercard and compliant with Site Data Protection (SDP) Program Level 1 service provider requirements. As each PCI Data Security Standard (PCI DSS) Attestation of Compliance (AOC) submitted to Mastercard is only valid for one year, it is important that service providers revalidate their compliance on time and submit their AOC annually to remain listed in good standing and avoid SDP noncompliance assessments due to expired validation.

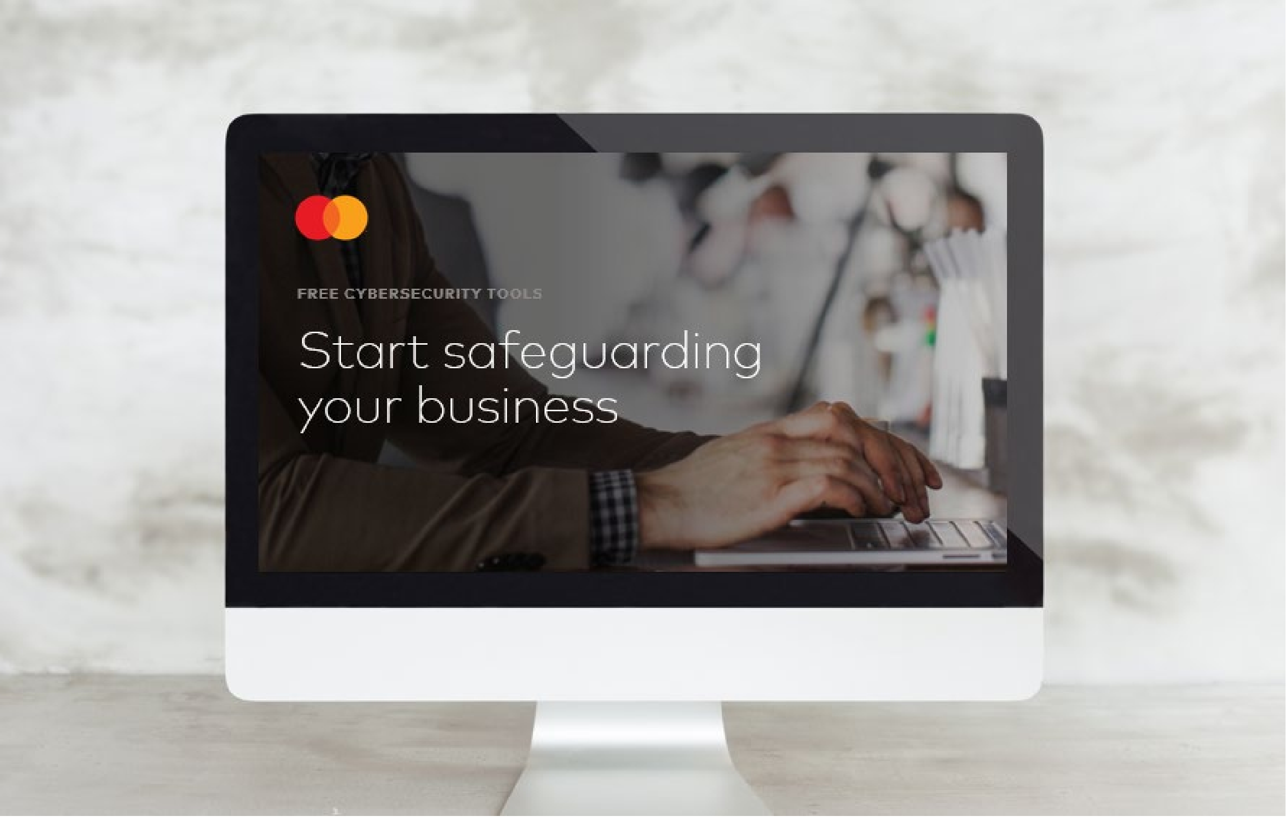
*Compromised Service Provider Delisting*

As a reminder, service providers that experience a breach or fail to cooperate in a forensic investigation will now be delisted from the Mastercard-approved service provider listing. A registered service provider may be placed back on the list only after they have re-validated compliance with the PCI DSS and has additionally demonstrated compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI DSS. The delisting of a compromised service provider will ensure that the approved listing contains up-to-date and accurate information.

*Cyber Standards & Programs FAQs Update*
The Cybersecurity Standards and Programs Frequently Asked Questions (FAQs) document, which currently consolidates commonly asked questions about Mastercard's existing PCI compliance programs under chapter 2 of the *Security Rules and Procedures*, will be replaced with three separate documents for easy navigation. The SDP Program FAQs, the Global Vendor Certification Program (GVCP) FAQs, and the Terminal and PIN Entry Security Standards FAQs will be updated and published shortly on the PCI 360 Educational Program resources website.

*Virtual Card Numbers & Compliance*
Mastercard SDP Standards require entities that store, transmit, or process account data to protect their customers' data in accordance with the PCI DSS. Since, PCI DSS applies to all primary account numbers (PANs) that represent a PCI Security Standards Council (PCI SSC) Participating Payment Brand, this would also include PANs that are provided electronically (virtual), not just those that correspond to a physical payment card. For more information on virtual card numbers (VCNs) issued for multiple use or single use (one-time only) purposes and their PCI DSS applicability, download the VCNs and SDP Compliance FAQs PCI 360 paper.

*PCI PTS HSM v2.0 Devices Expired 30 April*
PCI approval of devices validated against version 2.0 of the PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Requirements expired on 30 April. The PCI SSC has removed PTS HSM v2.0 devices from the PTS Approval list. This means that PTS HSM v2.0 devices cannot be newly deployed in the Mastercard acceptance network. Devices already deployed may continue to operate until Mastercard announces a sunset date but should be replaced as soon as feasible with an approved PCI PTS version.



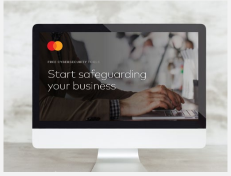
## MASTERCARD

### RESOURCES

Key Blocks FAQs

This new PCI 360 resource answers commonly asked questions about Mastercard's changes to support the PCI PIN Security Requirements and Testing Procedures involving phased key block implementations to meet security requirement 18-3.

Free Cybersecurity Program/Toolkit for Small Businesses



Learn how small businesses can defend their most important assets, business, and reputation through free online access to trusted cybersecurity resources and tools such as The Cyber Readiness Program and the Global Cyber Alliance (GCA) Cybersecurity Toolkit.

### EVENT

Europe Cybersecurity & Risk Summit: 3-6 Oct.

Mastercard's Europe risk summit will be held on 3-6 October in Venice, Italy. Join cybersecurity thought leaders in-person to discuss how your organization can minimize fraud risk and maximize profitability.

Become a sponsor.

*PCI PA-DSS v3.2 Retires 28 October*

The PCI Payment Application Data Security Standard (PA-DSS) v3.2 will retire on 28 October 2022. The standard will be formally replaced by the PCI Secure Software Standard and Program. Mastercard has already introduced the Software Security Framework (SSF) into SDP Program Standards. At this time, merchants and service providers that use any third party-provided payment applications or payment software must validate that each payment application or payment software used is listed on the PCI SSC's website as compliant.

*SDP Form due 30 Sept.*

The next merchant PCI DSS reporting form for Level 1-3 merchants, confirmed ADC merchants and merchants participating in either the PCI DSS Risk-based Approach or the PCI DSS Compliance Validation Exemption Program is due on 30 September. A new simplified version of the SDP Acquirer Submission and Compliance Status Form (SDP Form) will be available mid-July and should be used to report the PCI DSS compliance status of an acquirer's merchants. Acquirers with questions on merchant compliance or the revised SDP Form should send an email to the SDP Team.

## PCI Security Standards Council
## NEWS & UPDATES

*PCI DSS v4.0*

PCI DSS v4.0 was published on 31 March. Version 4.0 of the standard will replace v3.2.1 to address emerging threats and technologies and enable innovative methods to combat new threats. To provide entities time to understand the changes in v4.0 and implement any updates needed, the current version of PCI DSS, v3.2.1, will remain active for two years until it is retired on 31 March 2024. For more information on what has changed in the standard, download the Summary of Changes and the PCI DSS v4.0 At a Glance documents.

*PCI DSS v4.0 SAQs*

The PCI SSC has also published PCI DSS version 4.0 Self-Assessment Questionnaires (SAQs) and associated AOCs. Updates to the SAQs incorporate feedback received from the industry and includes changes such as: aligning requirement content with PCI DSS v4.0; adding new requirements to address evolving threats; rearranging, retitling, and expanding information in the introductory sections; and adding new appendices, as applicable, to support new reporting responses. PCI DSS v3.2.1 SAQs will remain active until PCI DSS v3.2.1 is retired in 2024.

*PCI PTS POI Modular Security Reqs. v6.1*

A minor revision to the PCI PTS Point-of-Interaction (POI) Modular Security Requirements was published in April. Version 6.1 of the standard incorporates PCI stakeholder feedback and comments received via a formal request for comment (RFC) period. Some of the changes in the revision include updated criteria on PAN truncation/encryption to accommodate 8-digit BINs, added criteria for use of unauthenticated wireless communications, and updated cryptographic check value language. The standard and supporting documentation can be accessed here.

*PCI 3DS v2.0 & Mobile Pymts on COTS RFCs*

Upcoming RFCs for the draft PCI 3-D Secure (3DS) Core Security Standard v2.0 and the draft Mobile Payments on Commercial off-the-shelf (COTS) ("MPoC") Standard, a new mobile standard designed to support the future evolution of mobile payments, are scheduled for this month and will close in July. Eligible PCI stakeholders are invited to review and provide feedback during a 30-day RFC period. Only comments that are submitted via the PCI SSC portal and received within the defined RFC period will be accepted. For additional information on the RFC process, download the RFC resource guide.

PCI COUNCIL

SSC HIGHLIGHTS

Resource Hub (DSS v4.0)

The new Resource Hub provides links to both standard documents & educational resources to help organizations become familiar with version 4 of the PCI DSS. Visit the hub for direct links to bulletins, blogs, videos, and more.

Coffee with The Council Podcast Series

Listen to the PCI SSC's new "Coffee with the Council" podcast series featuring PCI representatives discussing a variety of topics such as what to expect with DSS v4.0, assessor transition training, 2022 engagement opportunities, and regional perspectives.

Global Content Library—Coming in Nov.

The PCI SSC will debut a new global content library that will be available later this year (in November), which will provide a central location for members of the PCI community to access streamed online content. More to come…

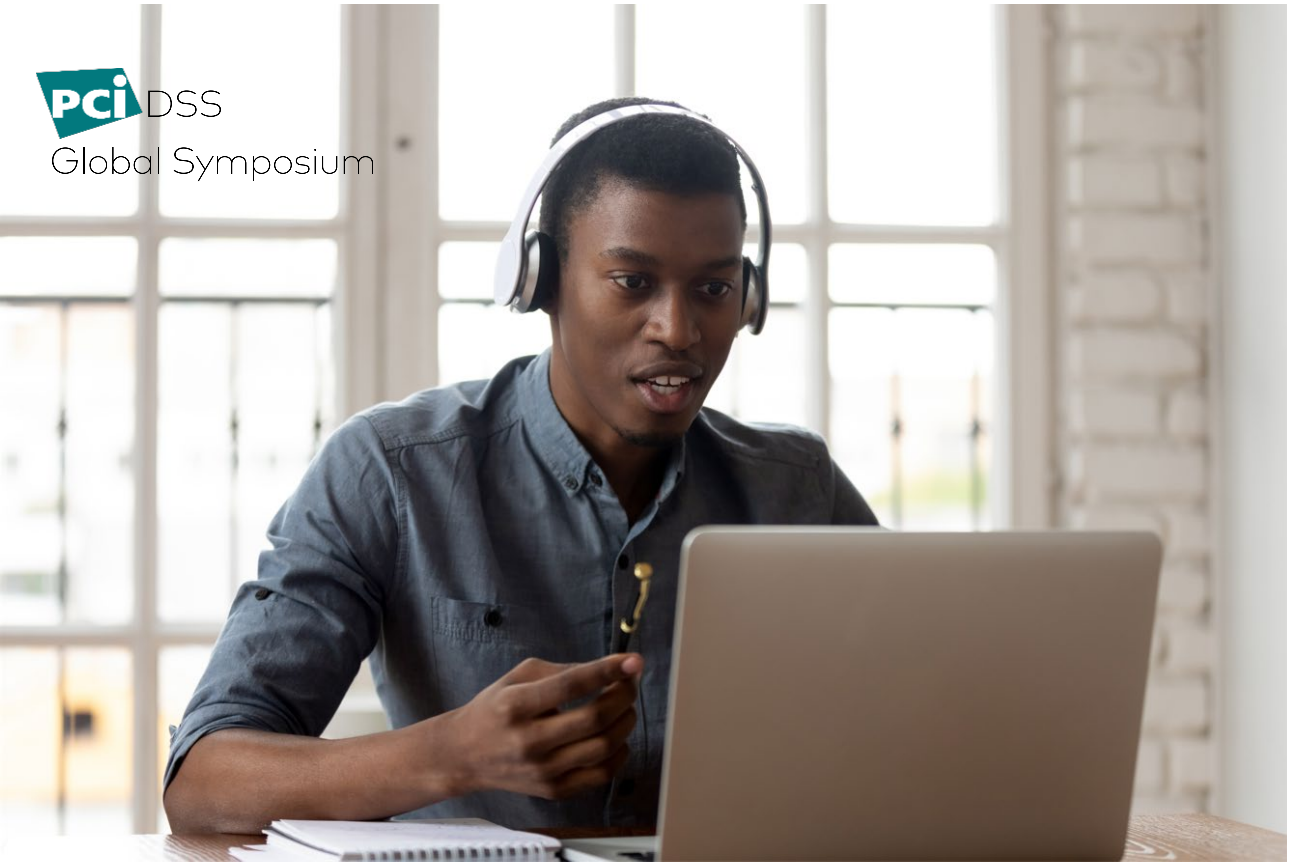
*2022 - 2024 GEAR Nominations*

The 2022 - 2024 Global Executive Assessor Roundtable (GEAR) nomination period is now open and will run through 24 June. GEAR allows senior executives of PCI assessor companies to provide advice, feedback, and guidance to the PCI SSC on the issues and concerns relating to assessments and assessor programs, including training content and qualification requirements, representing the perspectives of the PCI assessor community. PCI assessor primary contacts at eligible organizations can nominate senior executives as a candidate using the PCI SSC portal.

## EVENTS

*Community Program & Events*

Join the PCI SSC for a special online global program that will educate community members about the newly released PCI DSS v4.0. The PCI DSS v4.0 Global Symposium is scheduled to be released on 21 June and will be available on-demand until 30 August.  In addition, PCI SSC will be hosting regional face-to-face events this year in North America on 13-15 September in Toronto, Canada and in Europe on 18-20 October in Milan, Italy. For those that are not yet traveling, some event content and key sessions will be livestreamed.



## PCI COUNCIL

Get Involved

Join the community of Participating Organizations (POs) and play an active part in helping secure the future of payments.

TRAINING

In-Person/Remote Instructor-led eLearning

The PCI SSC now offers all PCI training programs as either in-person or remote instructor-led eLearning. The 2022 training schedule is now available through December.

View training FAQs.

Work from Home Security Awareness Training

This security awareness training course outlines many of the threats and challenges of handling and securing payment account data within home offices and remote working environments.