Q1 2022 PCI Quarterly Newsletter

Service Provider Validation

IN THIS ISSUE

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
REMINDERS

Service Provider PCI Compliance Validation
Annual PCI compliance validation is required for all Level 1 and Level 2 service providers registered with Mastercard. Each service provider must validate compliance to the Site Data Protection (SDP) Team by submitting the appropriate PCI Security Standard Attestation of Compliance (AOC) to pcireports@mastercard.com after initial registration and every year thereafter. For more information on service provider classifications and annual PCI compliance requirements, download the Service Provider Categories and PCI guidance paper.

Merchant PCI DSS Compliance Reporting
Merchant PCI Data Security Standard (DSS) compliance reporting for Level 1-3 merchants, confirmed account data compromise (ADC) merchants, and merchants participating in either the PCI DSS Risk-based Approach or the PCI DSS Compliance Validation Exemption Program is due on 31 March. Acquirers with Level 4 merchants in their portfolio are required to certify to Mastercard that they have a risk management program implemented but are not required to report Level 4 merchants via the semi-annual SDP Acquirer Submission and Compliance Status Form.

ADC Events Compliance Validation Deadlines
Merchants and service providers that experience a confirmed ADC Event are required to achieve full compliance with the PCI DSS within 60 calendar days after the conclusion of a forensic investigation performed by a PCI SSC Forensic Investigator (PFI). In addition, any compromised service provider must also demonstrate compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI DSS within twelve (12) months from achieving full compliance with the PCI DSS.

Noncompliance with the SDP Program
Noncompliance with the SDP Program could lead to the imposition of escalating assessments for Mastercard customers. Section 2.2 "Mastercard Site Data Protection (SDP) Program" in the *Security Rules and Procedures* describes the Program's implementation and PCI compliance validation requirements for customers with respect to their merchants and registered service providers, as well as potential assessments if those requirements are not met. It's important that customers remember to report/submit required PCI compliance validation when due for their merchants and service providers to avoid SDP noncompliance assessments.

8-Digit BIN Expansion & Truncation
As a result of industry changes to expand the Bank Identification Number (BIN) on payment cards from 6-digits to 8-digits of a primary account number (PAN), Mastercard's maximum allowable truncation format, "first 8, any other 4", will apply to all 16-digit PANs (regardless of BIN length). This approach was designed to simplify the PCI DSS assessment process for entities to meet SDP Program Standards and comply with the PCI DSS. For more information, download the 8-Digit BIN Expansion & PCI Standards PCI 360 paper or see the updated PCI SSC FAQ #1091 on acceptable formats for truncation.

MASTERCARD

PCI 360

Virtual Card Numbers & SDP Compliance FAQs

This new resource answers commonly asked questions about virtual card numbers (VCNs), such as multiple use-VCNs and single use-VCNs, as they relate to SDP Standards governed under Mastercard Cybersecurity Standards and Programs.

Terminal Servicers & SDP Compliance FAQs

This updated document is intended to assist customers and Terminal Servicers (TSs) on meeting SDP Program requirements and provides annual validation options for TSs that do not store, transmit, or process account, cardholder, or transaction data.

EVENT

Cybersecurity & Risk Summit: 11-14 April

Mastercard's North America risk summit will be held in-person on 11-14 April in Key Biscayne, Florida. If unable to travel, our live virtual experience will be held on 12-13 April. *Connect, collaborate, and share best practices with future partners & industry peers.*

PCI PA-DSS v3.2 Retires Oct. 2022

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.

PCI SECURITY STANDARDS COUNCIL

NEWS & UPDATES

PCI DSS v4.0 Release

PCI DSS v4.0 is scheduled to be released this month. The PCI DSS Report on Compliance (ROC) template and AOC will also be released at the same time, with the Self-Assessment Questionnaires following shortly thereafter. PCI DSS v3.2.1 will remain active for two years after v4.0 is published. The transition period from March 2022 until 31 March 2024 will provide organizations with time to become familiar with the changes in v4.0, update their reporting templates and forms, and plan for and implement changes to meet any updated requirements.

PCI PIN PTS HSM Requirements v4.0

The PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Security Requirements v4.0 was published in December. The updated standard ensures that HSM devices provide the strongest protection for critical data elements used in card verification, PIN processing, chip transaction processing, card personalization, secure cryptographic key loading, remote HSM administration and other payment authentication activities. Version 4.0 now includes the addition of a new evaluation module and approval class for evaluating cloud-based HSMs. Download the FAQs.

PCI Card Prod. & Provisioning Standard v3.0

The PCI Card Production & Provisioning Security Requirements v3.0 were published in January and ensures the strongest protections for customer information during card production and provisioning. The most significant change to the standard includes a new appendix for the use of a Security Operations Center (SOC) to control Security Management Systems to protect buildings, assets, access, and staff. Version 3.0 of the Card Production Logical and Physical reporting templates (ROC) and the Card Production Logical and Physical AOC templates will be published later this year.

Mobile Payments on COTS Standard RFC

The Mobile Payments on Commercial off-the-shelf (COTS) ("MPoC") Standard draft request for comments (RFC) period is now closed. Mobile Task Force members and PCI-Recognized Laboratories were invited to review and provide feedback from 24 January to 22 February 2022. The new mobile standard is designed to support the future evolution of mobile payments and builds on the existing PCI Software-based PIN Entry on COTS (SPoC) and PCI Contactless Payments on COTS (CPoC) Standards. A second RFC is scheduled for later this year. Stay tuned…

PCI Secure Software Standard—New Web Module RFC

The new Web Module for the PCI Secure Software Standard 30-day RFC period is open. The minor update introduces the "Web Software Module," which is a collection of supplemental security requirements for payment software intended for use in e-commerce or other internet-facing payment scenarios. The security requirements within the Web Software Module address common security issues related to the use of internet-accessible payment technologies that expose APIs for other entities or sites to access and use. The RFC is available to all Participating Organizations and technical contacts.

PCI COUNCIL

SSC HIGHLIGHTS

Bulletin: Ransomware Attacks Back on the Rise

Read the PCI SSC and the National Cybersecurity Alliance recent joint bulletin on the increasing threat of ransomware attacks on businesses & organizations and how to avoid becoming part of this increasing trend.

Bulletins: PCI PIN & P2PE Security Req. 18-3 Dates

Read these important bulletins published by the PCI SSC in Q2 2020 that addresses new effective dates for phased key block implementations included in the PCI PIN and Point-to-Point Encryption (P2PE) Security Requirement 18-3.

EVENT

PCI DSS v4.0 Global Symposium: 21 June

The PCI DSS v4.0 Global Symposium will be held on 21 June. This online event will help educate industry stakeholders about the newly released PCI DSS v4.0. See all PCI SSC's 2022 Community Events.