Q4 2021 PCI Quarterly Newsletter

DESV Validation Requirement

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
NEWS & REMINDERS

DESV for Compromised Service Providers

Effective 1 January 2022, Mastercard will require compromised service providers to demonstrate compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI Data Security Standard (PCI DSS) within 12 months from achieving full compliance with the PCI DSS. The new DESV requirement will help assess and document how service providers are maintaining compliance on a continual basis, 24/7, to protect against an Account Data Compromise (ADC) Event. For more information on revised standards, send an email to pci_adc@mastercard.com.

Compromised Service Provider Delisting from SDP Service Provider List

Service providers that experience a breach or fail to cooperate in a forensic investigation will be delisted from The Mastercard SDP Compliant Registered Service Provider List on the PCI 360 resources website, effective 1 January 2022. A registered service provider may be placed back on the list only after the entity has re-validated compliance with the PCI DSS and has additionally demonstrated compliance with the DESV. The delisting of a compromised service provider will ensure the approved listing contains up-to-date and accurate information.

Remote Assessment Guidelines Use
Mastercard will not require assessors to use the Remote Assessment Guidelines and Procedures, recently published by the PCI Security Standards Council (PCI SSC), when evaluating how organizations secure data. On-site assessments conducted by a PCI Qualified Security Assessor (QSA) should be completed wherever possible in accordance with applicable testing requirements and procedures. Where an on-site assessment is not possible, Mastercard recommends that assessors utilize the newly published guidance document when preparing for a remote assessment.

BIN Lengths & Truncation
As a result of upcoming 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 is designed to simplify the PCI DSS assessment process for entities to meet Site Data Protection (SDP) Program Standards and compliance with the PCI DSS. See the updated PCI SSC FAQ #1091 (November 2021) on acceptable formats for truncation.

Merchant PCI DSS Reporting due 31 March
The next merchant PCI DSS reporting 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 (Exemption Program) is due on 31 March 2022. As a reminder, acquirers with Level 4 merchants in their portfolio are required to have a L4 risk management program implemented but are not required to report their L4 merchants via the semi-annual reporting form. For more information on merchant compliance reporting or questions on an acquirer's L4 risk management program, acquirers can send an email to sdp@mastercard.com.

MASTERCARD

HIGHLIGHTS

8-Digit BIN Expansion & PCI Standards Paper

This new PCI 360 paper addresses commonly asked questions about the payments' industry migration to 8-digit BINs and provides clarification on the use of Mastercard's allowable truncation format to meet PCI DSS Req. 3.4.

Security Education & Awareness Videos

Watch these short videos to learn how cyber threats are becoming increasingly sophisticated and how important it is that organizations understand potential vulnerabilities and identify prevention and response strategies.

Phishing Prevention

Preventing Ransomware

ATM Cash-out Attacks

TRAINING

Cyber Basics Training for SMBs—Free

This free online training series is designed to assist small businesses with a series of basic practical steps that will help prevent the most common cyberattacks faced by small businesses on a daily basis. *Includes three 1-hour recorded webinar sessions.*

2022 SDP Form for Merchant Reporting
Mastercard will be revising the SDP Acquirer Submission and Compliance Status Form (SDP Form) for merchant PCI DSS reporting due 30 September 2022. The next version of the SDP Form will be available in Q2 2022 and updated to reflect revisions to SDP Standards which includes the introduction of the PCI Secure Software Standard, enhancements to the Exemption Program, revised Level 2 merchant PCI DSS compliance requirements, and upcoming changes to the PCI DSS v4.0 validation documents. Stay tuned for more to come…

PCI Security Standards Council
NEWS & UPDATES

PCI DSS v4.0 Preview
A draft version of PCI DSS v4.0 will be made available for Participating Organizations (POs), QSAs, and Approved Scanning Vendors (ASVs) in January 2022. The intent of the preview is to provide PCI SSC stakeholders additional insight into how version 4.0 of the standard is changing while it is being finalized for official release. The preview version in January will only be a draft. The final version of the PCI DSS v4.0 is scheduled for publication in March 2022 and may include additional revisions and modifications.

PCI DSS v4.0 Approach for MAFs and SAQs
In response to the request for comments (RFC) feedback received on the PCI DSS v4.0, the PCI SSC has decided to postpone further development of Merchant Assessment Forms (MAF) and will instead be updating the PCI DSS Self-Assessment Questionnaires (SAQ) to support the new standard as part of the March 2022 release. Publishing PCI DSS v4.0 SAQs will provide continuity for stakeholders that are used to completing SAQs, allowing them to focus on new requirements and other updates. The PCI SSC will continue to explore the MAF approach after version 4.0 of the standard and its supporting materials are published.

PCI P2PE v3.1 Published
The PCI SSC has published a minor revision to the PCI Point-to-Point Encryption (P2PE) Standard, which defines both security requirements and testing procedures for P2PE solutions and components. Revisions for PCI P2PE v3.1 include clarifications and updates previously released via technical FAQs and bulletins, corrections to proofing errors, and responses to stakeholder comments. The updated standard also incorporates changes made in the PCI PIN Security Standard v3.1 published earlier this year. PCI P2PE v3.1 and supporting documents can be found here.

Ransomware Attacks
Ransomware is the fastest growing malware threat. Ransomware attacks are becoming an increasing trend that has been front and center in the news recently due to high-profile breaches that have impacted many businesses. With a dramatic increase in security challenges due to the disruptions caused in part by the COVID-19 pandemic, there has been a significant increase in number of attacks across the globe. For more information on key considerations and educational resources to help protect against these cyberattacks, download the PCI SSC's ransomware infographic.

PCI Card Prod. & Provisioning Standard v3.0
The PCI Card Production & Provisioning Security Requirements v3.0 is nearing completion and should be published in Q1 2022. Version 3.0 of the standard ensures the strongest protections for customer information during card production and provisioning. The most significant change to the standard includes the addition of new security requirements for a Security Operations Center in Appendix C. A Security Operations Center is optional and when implemented provides a centralized location to manage and operate the CCTV, Access Control and Alarm Systems for multiple facilities.

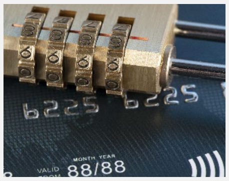
PCI COUNCIL

SSC RESOURCES

PCI PTS PIN Security Reqs. Technical FAQs

Read the new FAQs published in the PCI PTS PIN Security Requirements Technical FAQs that describe what fixed key & master key/session key management is to meet the PCI PIN Standard effective date 1 January 2023.

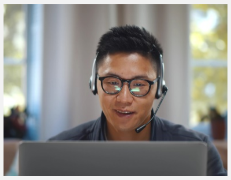
Implementing ISO Format 4 PIN Blocks Information Supplement



This document provides guidance to help PIN acquiring entities with the planning, migration, and testing of the implementation of ISO Format 4 PIN blocks in conformance with the reqs. in the PCI PIN Standard.

TRAINING

2022 Training Schedule



The 2022 training schedule is now available through June. The PCI SSC offers a variety of training and qualification programs via eLearning with remote exam delivery (computer-based training + live remote instructor-led training).