# Q4 2020 PCI Quarterly Newsletter

## IN THIS ISSUE

MASTERCARD

NEWS & REMINDERS

LATEST RESOURCES

PCI COUNCIL

NEWS & UPDATES

SSC RESOURCES

TRAINING

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

## Mastercard
## NEWS & REMINDERS

*PCI Software Security Framework Standards*

Mastercard will be introducing the PCI Software Security Framework (SSF) into Site Data Protection (SDP) Program Standards in Q1 2021. This means all merchants and service providers that use third party-provided payment applications or payment software must either validate that each one is compliant with the PCI Payment Application Data Security Standard (PA-DSS) or the PCI Secure Software Standard, as applicable. It will also be strongly recommended that merchants and service providers only use software vendors that comply with the PCI Secure Software Lifecycle (Secure SLC) Standard.

*PCI PA-DSS Transition to SSF*

When the PA-DSS v3.2 expires in October 2022, the standard will be formally retired and replaced by the PCI SSF which supports a broader array of payment software types and technologies. To help understand and plan ahead for this transition, Mastercard recommends that customers and their merchants and service providers review the PCI SSC's Software Security Framework FAQs document which addresses key questions related to the SSF, including its impact to PA-DSS validated applications and how PA-DSS will be phased out.

*Account Testing Attacks*

The threat of account testing attacks to payment security is becoming a growing trend. An account testing attack - also referred to as BIN attack - involves a cybercriminal testing payment account numbers in order to validate cardholder information. Once an account number is validated, it can then be monetized by being sold on the Dark Web or utilized to commit fraudulent transactions. Mastercard is encouraging customers and their merchants to review the PCI SSC's and the National Cyber-Forensics and Training Alliance's (NCFTA) recent bulletin on defending against these types of attacks.

*ATM Cash-Out Attacks*

ATM cash-out attacks also continue to be an ongoing threat globally. These attacks often insert malware via phishing or social engineering methods into a financial institution or payment processor's card management systems altering the fraud prevention controls such as withdrawal limits or PIN number of compromised cardholder accounts. Mastercard is notifying customers and payment processors of this growing concern and recommends reviewing the PCI SSC's and the ATM Industry Association's (ATMIA) guidance and information on protecting against ATM cash-outs.

*Cybersecurity Training*

Free online cybersecurity educational training for issuers and merchants is now available on PCI 360. The Issuer Cyber Training is designed to provide a high-level overview of ATM cash-out attacks and best practices to defend against these types of cyber attacks while the Merchant Cyber Training offers small merchants with an overview on what cybersecurity is, PCI DSS goals and requirements and what to expect if a data breach occurs. The trainings are available in English, Portuguese and Spanish. Access the trainings here.

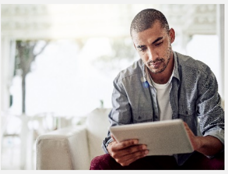
*Option for L2 DSE Service Providers*

Mastercard has revised SDP Standards to allow an alternative option for qualifying Level 2 Data Storage Entities (DSEs) to validate compliance. A L2 DSE may submit a

MASTERCARD

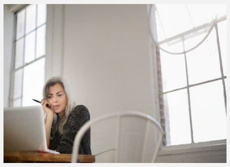
LATEST RESOURCES

3 Myths About PCI Compliance



Listen to SecurityMetrics podcast with John Elliott, Director of Industry Standards at Mastercard, who reveals the three biggest myths about PCI DSS compliance that cost you time and how they hinder security.

Cybersecurity Standards and Programs FAQs



The PCI 360 document highlights commonly asked questions about Mastercard's Cybersecurity Standards and Programs for customers, merchants, service providers and card production vendors.

Terminal & PIN Entry Security Standards FAQs

This frequently asked questions document is designed to help acquirers and merchants with Mastercard security standards applicable to terminals such as ATM and POS terminals, including PIN entry standards.

PCI PIN Security Requirements Attestation of Compliance (AOC) for Onsite Assessments from a PCI SSC-approved Qualified PIN Assessor (QPA) to the SDP Team instead of the PCI Data Security Standard (PCI DSS) AOC, provided that they do not perform services involving the storage, transmission, or processing of account, cardholder, or transaction data. Read the updated Service Provider Categories & PCI document.

*SDP Registered Service Provider List Move*
The Mastercard SDP Compliant Registered Service Provider List has been moved to the PCI 360 Education Program site in order to consolidate all SDP and PCI 360 resources onto a single platform. The SDP Compliant Registered Service Provider List provides information on service providers that are registered with Mastercard and compliant with SDP Program Level 1 service provider requirements (an annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor [QSA]). Merchants and service providers can still access the list by visiting the SDP Service Provider page or the SDP Merchant page on www.mastercard.com.

*SDP Form due 31 March*
The next SDP Acquirer Submission and Compliance Status Form for Level 1, Level 2, and Level 3 merchant PCI DSS compliance reporting to Mastercard will be due on 31 March 2021. As a reminder, an acquirer must 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 or download the *Security Rules and Procedures – Merchant Edition* manual here.

## PCI Security Standards Council
## NEWS & UPDATES

*PCI Secure Software Lifecycle Standard*
The PCI Secure SLC Standard provides security requirements for payment software vendors to integrate security throughout the entire software lifecycle, which results in software that is secure by design and able to withstand attacks. It is intended for vendors that are developing payment software that supports and facilitates payment transactions. Vendors can learn more about the standard, what it is and the value of adoption by reading the SSF at-a-glance document: PCI Software Security Framework Provides a Modern Approach to Payment Software Security.

*COVID-19 Impact on PCI P2PE Revalidations*
COVID-19 restrictions have impacted annual point-to point encryption (P2PE) revalidations and 3-year reassessments of P2PE Solutions, P2PE Components and P2PE Applications. As a result, the PCI SSC is extending the allowances previously communicated for P2PE products due for annual revalidation or reassessment before 30 June 2021. Vendors requesting an extension are required to submit an attestation to confirm their ongoing adherence to the PCI P2PE Standard. For more information on extension requests, contact P2PE@pcisecuritystandards.org.

*PCI PIN & P2PE Security Req. 32-9 Dates*
Based on industry feedback, the PCI SSC has published bulletins revising implementation dates on encrypted key loading included in PIN and P2PE Security Requirement 32-9: *The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD.* The new implementation dates are effective immediately and will be reflected in the PCI PIN Security Requirements and Testing

PCI COUNCIL

SSC RESOURCES

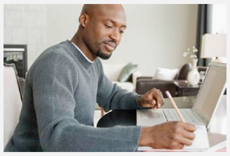
PCI Software Security Framework Overview

The PCI SSC's *at-a-glance* document provides an overview on how SSF replaces the PA-DSS with modern requirements that support a broader array of payment software types and technologies.

PCI PIN Security—Case Studies

Read the PCI PIN Security in Practice Case Studies: First Tech and Gertec, Brazil Regional Engagement Board Members, to learn how PIN Security requirements help organizations with properly implementing PCI PIN security controls.

Protecting Payments Data During COVID-19



As circumstances evolve, a variety of issues including the impact on assessments, trainings and keeping payment data secure have arisen. The *PCI Perspectives blog* offers guidance and resources on many of these topics.

Procedures v3.1 due for release later this year, and in a technical FAQ for the time being until the P2PE Standard is updated.

*Participating Organizations Survey*
The PCI SSC is seeking feedback from Participating Organizations (POs) to ensure the program continues to meet the needs of the industry. POs can help PCI SSC best support your organization by completing a short survey. As a global forum, POs bring together payments industry stakeholders to develop and drive implementation of data security standards and resources for safe payments worldwide. For more information on joining the PO Program or learning more about the benefits and opportunities of becoming a PO, send an email to participation@pcisecuritystandards.org.

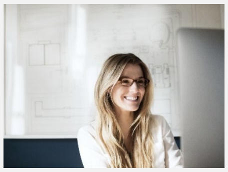
*2021 SIG Election*
Now through 21 December, POs are invited to vote on proposals for 2021 Special Interest Group (SIG) projects. PCI SSC stakeholders can vote on one of five proposed topics by logging on to the PCI portal. The results of the SIG election will be shared in January 2021. SIGs are community-driven initiatives that focus on payment security challenges related to PCI Security Standards. They bring together experts from across industries and around the world to address topics that are most important to payment security efforts.

**TRAINING**
*2021 Training Schedule—Online Certification*
The PCI SSC has announced the eLearning training schedule through June 2021. The training classes and the exams will be conducted as remote Instructor Led Training (ILT). The classes will be a combination of computer-based training as well as an instructor-led session that must be completed prior to the exam. The exam will also be delivered remotely using a proctoring service or can be taken at a local Pearson Vue location, if available.

## PCI COUNCIL

SSC RESOURCES *(cont.)*

Women in Payments Blog Series



Listen to this monthly award-winning Q&A blog series to hear women cybersecurity experts discuss their career as well as provide guidance on how to develop a career path in the industry.

TRAINING

eLearning Available On-Demand

The PCI SSC offers a variety of training and qualification programs via eLearning on-demand. Acquirer, Internal Security Assessor (ISA) and Qualified Integrators & Resellers (QIR) training classes are available anytime you are.

Wishing You
Happy Holidays
from the Mastercard
SDP Team