Q1 2019 PCI Quarterly Newsletter

IN THIS ISSUE

MASTERCARD

NEWS & REMINDERS

L4 Risk Management Program Deadline

This month is the deadline for acquirers to certify to Mastercard that they have a risk management program in place to identify and manage security risk within their Level 4 merchant portfolio. An additional question has been added to the SDP Acquirer Submission and Compliance Status Form (SDP Form) for acquirers to attest to having one implemented by 31 March 2019. For more information on this important deadline, download Guidance for Level 4 Merchant Risk Management Program.

PCI Data Security Essentials for SMBs

Mastercard has incorporated PCI Data Security Essentials Resources for Small Merchants and the new Evaluation Tool into SDP Program Standards as additional guidance tools to use while working towards PCI DSS compliance. These useful resources provide security basics for small merchants to protect against payment data theft and to help simplify their security and reduce their risk. *Note—A Level 4 merchant that only completes the Evaluation Tool is not PCI DSS compliant. A Level 4 merchant may validate compliance using the validation tools described in section 10.3.2 of the Security Rules and Procedures.*

SDP Form due 31 March

The next SDP Form for Level 1, Level 2, and Level 3 merchant compliance reporting is due on 31 March. Acquirers should download

the latest version of the form, V5.0, complete it in its entirety and submit it on-time to avoid potential noncompliance assessments for late reporting/non-reporting. For more information on the next SDP Form submission deadline, merchant compliance validation requirements, or questions on the Level 4 risk management program certification, acquirers can send an email to sdp@mastercard.com. See also SDP FAQs.

PCI DSS Validation Exemption Program
Mastercard offers Level 1 and Level 2 merchants using secure payment technologies such as EMV chip or a validated point-to-point encryption (P2PE) solution an alternative way to validate SDP compliance. Participation in the PCI DSS Compliance Validation Exemption Program eliminates the requirement to validate PCI DSS compliance annually. Acquirers are encouraged to work with their merchants to see if they meet all eligibility requirements of the program. *Note—Level 4 merchants are eligible to participate.*

L1-2 Service Provider Annual Validation
The SDP team is reminding customers that compliance validation is required annually for Level 1 and Level 2 service providers registered with Mastercard. The PCI Attestation of Compliance (AOC) and latest ASV Scan AOC must be submitted to pcireports@mastercard.com after initial registration and every year thereafter. If a newly registered service provider is not yet compliant, the PCI Action Plan is required to be completed and submitted for review. For more information on service provider compliance validation requirements, download the Service Provider Categories and PCI Guidance paper.

Requirement Changes Ahead for QSAs
The PCI Security Standards Council (SSC) is increasing the professional certifications requirement for Qualified Security Assessors (QSAs). Current requirements note that QSAs must hold an information security certification or an IT audit certification. Going forward, QSAs will maintain two industry certifications, one information security and one IT audit certification. This requirement was effective 1 January 2019 for new QSAs and will be effective 1 July 2019 for QSAs qualified and listed prior to 1 January 2019. Entities should check that their QSA meets the new industry requirement. See QSA FAQs.

PCI DSS V3.2 Now Retired
The PCI DSS V3.2 was retired on 1 January 2019. Merchants and service providers must now validate PCI DSS compliance with V3.2.1 that was published in May 2018. While organizations were given six months to complete their transition from V3.2, it is important for merchants and service providers that have not yet transitioned between PCI DSS V3.2 and V3.2.1 to complete their transition to the latest version of the standard as soon as possible. The SDP team will only accept validations to V3.2.1. PCI DSS V3.2.1 supporting documents (updated reporting templates and forms) can be found on the PCI SSC's website.

EVENTS

Americas Risk Conference
Mastercard's annual Americas Risk Conference is taking place at The Westin Hilton Head Island Resort & Spa on 6-9 May in Hilton Head, South Carolina. Join the Global Risk Leadership team and industry experts who will share the latest updates on securing commerce by leveraging strong authentication, intelligence and technology to address the latest cyber threats, the role of Artificial Intelligence in reducing fraud and risk, and biometrics and the importance of digital identity. Do not forget to register for pre and/or post-conference workshops (like the *Cybercrime & Payments Security* workshop) led by subject matter experts.

PCI 360

Download Mastercard's PCI 360 Educational Resources

Terminal and PIN Security FAQs - Coming Soon

This new document will assist acquirers and their merchants with frequently asked questions on compliance and validation requirements for Mastercard's Terminal and PIN Security Standards.

EVENTS

Secure the Payments Ecosystem through Innovation and Collaboration

Americas Risk Conference - Hilton Head, SC, USA 6–9 May

LAC Fraud Management Forum – Orlando, FL, USA 18-20 June

View the agenda.

LAC Fraud Management Forum
The LAC Fraud Management Forum is taking place at the Hilton Orlando Bonnet Creek on 18–20 June in Orlando, FL. The Regional Fraud Management Forum brings together experts from the payments media industry. Join the Mastercard Latin American and Caribbean team for an event filled with networking, sharing, and learning about security in the digital space, authentication in electronic commerce, effective management of authorizations, tokenization and much more. *The forum will be held in Spanish only.*

PCI Security Standards Council
NEWS & UPDATES

PCI 3DS SDK Standard V1.1
Version 1.1 of the PCI 3D Secure Software Development Kit (3DS SDK) Standard was published in December. The minor revision provides more detailed assessment procedures and guidance for PCI 3DS SDK Labs performing 3DS SDK security evaluations. The PCI 3DS SDK Security Standard supports the EMV® 3-D Secure SDK Specification that defines EMV 3DS requirements for entities developing 3DS SDKs for use in mobile-based 3DS transactions. Read What's New in PCI 3DS SDK Security Standard Version 1.1?

PCI Software Security Standards
In January, the PCI SSC published new requirements for the secure design and development of modern payment software. The PCI Secure Software Standard and the PCI Secure Software Lifecycle (Secure SLC) Standard are part of a new PCI Software Security Framework, which will also include a validation program for software vendors and their software products, and a qualification program for assessors. The programs will be launched later this year. Read Just Published: New PCI Software Security Standards.

PCI Contactless Payments on COTS Standard Update
Efforts are underway to develop a security standard for accepting contactless payments on a merchant's commercial off-the-shelf (COTS) phone or tablet. The intent is to develop security requirements for

PCI COUNCIL

Get Involved to Make Payments Safer

Join the PCI SSC Participating Organization Program to help secure payment data.

SSC RESOURCES

Best Practices for Maintaining PCI DSS Compliance

This information supplement provides updated guidance and practical recommendations for dealing with the challenges associated with maintaining PCI DSS compliance (replaces SIG guidance previously published in August 2014). Read blog.

FAQ 1443: What is the Intent of the SAQ Eligibility Criteria?

This FAQ notes that in order for a merchant environment to meet SAQ eligibility criteria, only system types defined in the eligibility criteria may be used in that environment. *Merchants should always consult with their acquirer to determine which SAQ is appropriate for their environment.*

solutions that enable a merchant's COTS device to accept contactless payments without the need for a dongle or other type of peripheral reader by leveraging near-field communication (NFC) capabilities inherent to a COTS phone or tablet. The PCI SSC is planning a request for comments (RFC) period for later this month. Read PCI SPoC and Contactless Standards: What to Expect in 2019.

RFC Process
The PCI SSC has launched a more formal process for soliciting feedback on existing and new PCI Security Standards through the Request for Comments process. Depending on the RFC topic, stakeholders may include Subject Matter Experts (SME), Participating Organizations (PO), applicable assessors, Approved Scanning Vendors (ASV), the Board of Advisors, PCI labs, vendors, task force members, and others. This feedback plays a critical role in the ongoing maintenance and development of these resources for the payment card industry. Download the RFC Process Guide or view the RFC-at-a-Glance infographic.

SPoC Annex RFC
A PCI SPoC Magnetic Stripe Reader (MSR) Annex is currently in the development stages. The PCI SPoC MSR Annex will outline the security and testing requirements needed to ensure the protection of account data accepted through SPoC solutions that support magnetic stripe transactions. POs are invited to review and provide feedback on the draft SPoC MSR Annex during a 30-day RFC period through the PCI portal. All feedback will be reviewed and considered for development of the final Annex which is planned for publication in May. The PCI SSC will incorporate the Annex into the SPoC Standard as part of a revision anticipated for 2020.

2019-2020 Board of Advisors
The 2019-2020 Board of Advisors was announced end of January. One of the best ways for POs to ensure their issues and perspectives are heard is through representatives on the Board of Advisors. The Board provides PCI SSC leadership with critical visibility and insights into the payment security challenges and opportunities facing the industry. The PCI SSC relies on this input to develop data security standards and programs that help businesses globally detect, mitigate and prevent cyberattacks and breaches.

Brazil Regional Engagement Board
PCI SSC has announced a newly expanded 2019 Brazil Regional Engagement Board. Additional seats have been added to make room for those companies that were nominated for the inaugural board but weren't selected and to include service providers which are an important and growing segment in the Brazil payment card industry. The Brazil Regional Engagement Board members serve as advisors to the PCI SSC on regional payment data security issues and represent the perspectives of key stakeholders in Brazil. Read the blog.

QPA Program
The PCI PIN Assessor program to train and qualify security assessors to support the implementation of the PCI PIN Security Standard was launched end of January. This new program will certify security professionals to perform assessments using the PCI PIN Security Standard. New instructor-led training and quality management processes are being developed to support the program. PCI SSC will list Qualified PIN Assessor (QPA) Companies and their certified employees on its website. The use of QPAs will be determined by the payment brands. Download the QPA program documents.

2019 SIG Project
The Special Interest Group (SIG) project topic selected for 2019 will be: *PCI DSS*

PCI COUNCIL

TRAINING

The PCI SSC offers a variety of training and re-qualification courses in eLearning and instructor-led formats.

Acquirer Training

Acquirers can take a six-hour eLearning training to improve their skill level and provide their merchants with a higher level of advice.

Merchant Training

The PCI SSC offers a range of merchant training and certification programs to support businesses in their payment security efforts.

Qualified Integrators & Resellers (QIR) Training

The QIR course provides guidelines, training and qualification on the most critical control areas related to the installation of payment systems into merchant environments.

For more information on PCI training courses, send an email to the PCI SSC at training@pcisecuritystandards.org or download Training Programs at a Glance.

assessments in large organizations. The SIG will consider issues such as how PCI DSS assessments can be logically broken down and the impact of any dependencies as well as helping large organizations recognize their assessments may include legal entities in various jurisdictions. The SIG is set to kick off this month. Interested organizations are encouraged to sign up to participate by emailing sigs@pcisecuritystandards.org. View recent SIG guidance.

EVENTS

India Forum

The PCI SSC will be holding it's first-ever Forum in India this month at the Hyatt Regency Delhi on 13 March in New Delhi, India. The forum will bring together regional community figures and merchants. Plan on joining the PCI SSC for a day of networking opportunities, updates on industry trends, insights and strategies on best practices, engaging keynotes and industry expert speakers. Don't forget to meet with Mastercard's PCI SSC representatives who will be onsite too. View the agenda here.

Acquirer Forum

The PCI SSC Acquirer Forum will take place at the Mandalay Bay on 30 April in Las Vegas, Nevada. The forums help bring together payment processors and acquiring banks around the world to share information and discuss challenges and solutions for improving payment security. The Acquirer Forums feature updates from the PCI SSC on key initiatives as well as external speakers to provide insight and intelligence into the payment security landscape that will help you and your customers protect payment card data. Register for the Acquirer Forum.

EVENTS

Attend the 2019 Community Meetings and Forums where the PCI SSC staff and industry experts will share the latest payment security updates.

India Forum – New Delhi, India 13 March

Acquirer Forum – Las Vegas, NV, USA 30 April