Site Data Protection (SDP) Program

Frequently Asked Questions

1 August 2018

Notices

Following are policies pertaining to proprietary rights and trademarks.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

In the event of a conflict between the information contained in this document and the Mastercard Standards, the Standards are afforded precedence.

Summary of SDP Program Changes - *Global Operations Bulletin* No. 3, 1 March 2017

The below table reflects 2017 SDP Program changes included in this *Frequently Asked Questions* document. For more information on Mastercard SDP Program rules, review 10.3 of the *Security Rules and Procedures Manual* on Mastercard Connect™ or click here to access the Merchant Edition of the manual.

10.3 Mastercard Site Data Protection (SDP) Program Changes
• Mastercard no longer requires an acquirer to report merchant PCI DSS compliance to Mastercard on a quarterly basis. An acquirer will submit the completed SDP Acquirer Submission and Compliance Status Form via e-mail to the SDP mailbox (sdp@mastercard.com) twice per year on 31 March and 30 September. • Level 1 and Level 2 Merchants located outside of the U.S. region may qualify as compliant with the Mastercard PCI DSS Risk-based Approach by validating compliance with the first two of six total milestones of the PCI DSS Prioritized Approach. • Mastercard has expanded the qualification criteria for the Mastercard PCI DSS Compliance Validation Exemption Program as follows: – Include Level 4 Merchants as eligible participants – For a Level 1, Level 2, or Level 4 Merchant that does not have at least 75 percent of its annual total acquired Mastercard and Maestro transaction count processed through hybrid point-of-sale (POS) terminals, the merchant will still be qualified if it has implemented a validated point-to-point encryption (P2PE) solution listed on the PCI Security Standards Council (SSC) website. • Mastercard recommends that Level 1 and Level 2 Service Providers demonstrate to Mastercard their compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI DSS. • Level 3 and Level 4 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved Qualified Security Assessor (QSA) for an onsite assessment instead of performing a self-assessment. • Effective 31 March 2019, an acquirer must certify to Mastercard via the updated SDP Status Form that it has a risk management program in place to identify and manage payment security risk within the acquirer's Level 4 Merchant portfolio. • Mastercard recommends that a Merchant (regardless of level) use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website to implement a payment application compliant with the *PCI Payment Application DSS* (PCI PA-DSS).

Frequently Asked Questions – SDP Program Changes, 1 March 2017

Frequently Asked Questions – Other

Q: What is the Mastercard Site Data Protection (SDP) Program?

The SDP Program is Mastercard's program in support of PCI Security Standards and is designed to encourage customers, merchants, and Service Providers to protect against Account Data Compromise (ADC) Events. The SDP Program promotes the identification and correction of vulnerabilities in security processes, procedures, and website configurations.

Q: Who is required to comply with the PCI DSS?

Compliance with the PCI DSS is required for all issuers, acquirers, merchants, Service Providers and any other entity that stores, processes or transmits Mastercard and Maestro account data.

Q: Who is required to validate/report their PCI DSS compliance to Mastercard?

The SDP Program requires validation of compliance only for merchants and Service Providers.

Q: I am an acquirer or an issuer. Do I need to validate/report compliance to Mastercard?

Acquirers and issuers are required to achieve PCI DSS compliance, however, an acquirer or an issuer does not have to report their PCI DSS compliance to Mastercard.

Q: I am a merchant. What do I need to do to meet SDP Program requirements?

Mastercard recommends that you contact your acquiring bank to assist you with:

- Determining your merchant level (L1, L2, L3 or L4) based on combined annual Mastercard and Maestro transaction counts
- Confirming PCI DSS compliance validation requirements

It is your acquirer who will manage your PCI DSS compliance and report your status directly to Mastercard. Mastercard does not accept PCI DSS validation documentation sent by a merchant.

A merchant that stores, processes or transmits cardholder data must be PCI DSS compliant and a merchant that uses third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PA-DSS).

2017 UPDATE

Mastercard recommends that a merchant (regardless of level) use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website to implement a payment application compliant with the PCI PA-

DSS. QIRs are organizations qualified by PCI SSC to implement, configure and/or support PA-DSS validated payment applications on behalf of merchants.

For more information on merchant compliance requirements, review 10.3 of the *Security Rules and Procedures Manual – Merchant Edition*.

Q: I am an acquirer. What do I need to do to meet SDP Program requirements?

An acquirer is responsible for implementing a PCI DSS compliance program for their L1, L2, L3 and L4 merchants. To ensure compliance with the SDP Program, you should:

- Help determine merchant levels based on combined annual Mastercard and Maestro transaction counts
- Review and communicate merchant compliance validation requirements for each L1, L2, L3 and L4 merchant in your portfolio
- Set deadlines for merchants to submit PCI DSS validation documents
- Submit a completed SDP Acquirer Submission and Compliance Status Form[1] to sdp@mastercard.com reporting on your merchants' PCI DSS compliance status *(only L1, L2 and L3 merchants are required to be reported via the SDP Form. L4 merchant reporting to Mastercard is optional.[2])*

2017 UPDATE

[1] Mastercard no longer requires an acquirer to report merchant PCI DSS compliance to Mastercard on a quarterly basis. An acquirer must submit the completed SDP Acquirer Submission and Compliance Status Form via email to the SDP mailbox (sdp@mastercard.com) twice per year (semi-annually) on 31 March and 30 September.

[2] Effective 31 March 2019, an acquirer must certify to Mastercard via the SDP Acquirer Submission and Compliance Status Form that it has a risk management program in place to identify and manage security risk within the acquirer's Level 4 Merchant portfolio. An additional - yes or no - question has been added to the SDP Acquirer Submission and Compliance Status Form for acquirers to attest to having a risk management program in place for their Level 4 Merchants.

For more information on acquirer compliance requirements, review 10.3 of the *Security Rules and Procedures Manual* on Mastercard Connect™ or send an email to sdp@mastercard.com.

Q: I am a Service Provider. What do I need to do to meet SDP Program requirements?

Mastercard recommends that you review SDP Program requirements to assist with:

- Determining your Service Provider level (L1 or L2) based on combined annual Mastercard and Maestro transaction counts
- Confirming PCI DSS compliance validation requirements
- Once compliant, submit a signed Attestation of Compliance (AOC); or for those SAQ eligible, submit the SAQ D AOC and latest passing scan to pcireports@mastercard.com.

- If not yet compliant, the PCI Action Plan for Service Providers should be completed and submitted to pcireports@mastercard.com.

A Service Provider that stores, processes or transmits cardholder data must be PCI DSS Compliant and a Service Provider that uses third party-provided payment applications must only use payment applications that are compliant with the PA-DSS.

To be listed on *The Mastercard SDP Compliant Registered Service Provider List* updated monthly on the SDP website, a Service Provider must have submitted to pcireports@mastercard.com a copy of their AOC by a QSA reflecting validation of the company being PCI DSS compliant and been registered as a Service Provider by one or more Mastercard Customers.

Note: Service Provider classifications (for example TPP, DSE, PF, SDWO, DASP, TSP, TS, or 3-DSSP) is determined by the Mastercard Service Provider Registration Team (service_provider@mastercard.com).

2017 UPDATE

Mastercard recommends that Level 1 and Level 2 Service Providers demonstrate to Mastercard their compliance with the PCI DSS Designated Entities Supplemental Validation (DESV) - appendix of the PCI DSS. The DESV tool provides additional criteria for demonstrating how PCI DSS controls are being applied continuously to protect payment data from compromise.

An additional field (checkbox) has been added to *The Mastercard SDP Compliant Registered Service Provider List* to show those Service Providers that demonstrate compliance with the DESV.

For more information on Service Provider compliance requirements, review 10.3 of the *Security Rules and Procedures Manual – Merchant Edition*.

Q: I am a SDP Level 1 Merchant. What are my PCI compliance validation requirements?

To validate compliance, a L1 merchant must successfully complete:

- An annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA) or internal auditor
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

A L1 merchant that uses an internal auditor for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the PCI DSS attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue to use an internal auditor.

Q: I am a SDP Level 2 Merchant. What are my PCI compliance validation requirements?

To validate compliance, a L2 merchant must successfully complete:

- An annual self-assessment conducted by an Internal Security Assessor (ISA) or may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

A L2 merchant must ensure that staff engaged in self-assessing the merchant's compliance with the PCI DSS attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue the option of self-assessment for compliance validation.

Q: I am a SDP Level 3 Merchant. What are my PCI compliance validation requirements?

To validate compliance, a L3 merchant must successfully complete:

- An annual self-assessment
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

Note: A L3 merchant completing a Self-Assessment Questionnaire (SAQ) should consult with their acquirer to determine which SAQ is appropriate for their environment.

2017 UPDATE

Level 3 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

Q: I am a SDP Level 4 Merchant. What are my PCI compliance validation requirements?

A merchant that is not deemed to be a L1, L2, or L3 merchant is a L4 merchant. While a L4 merchant is not required to validate/report their PCI DSS compliance to Mastercard, a L4 merchant is still required to be PCI DSS compliant and must successfully complete:

- An annual self-assessment
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

Note: A L4 merchant completing a Self-Assessment Questionnaire (SAQ) should consult with their acquirer to determine which SAQ is appropriate for their environment.

2017 UPDATE

Level 4 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

Q: Are there alternative ways to validate PCI compliance to Mastercard if I use secure technology such as EMV or P2PE?

Mastercard offers a merchant implementing secure technologies such as EMV or P2PE alternative ways to validate their PCI DSS compliance. A qualifying merchant may validate compliance through either the *Mastercard Risk-based Approach*[1] (applies to eligible non-U.S. merchants only) or the *Mastercard PCI Compliance Validation Exemption Program (the "Exemption Program")*[2] (applies to eligible merchants in all Regions).

Both the Risk-based Approach and PCI Compliance Validation Exemption Program provide some validation/reporting relief to merchants. Mastercard encourages you to review 10.3.4.1 Risk-based Approach and 10.3.4.2 PCI Compliance Validation Exemption Program in the *Security Rules and Procedures Manual – Merchant Edition* for more information on eligibility requirements. A merchant that does not satisfy all eligibility criteria must continue to validate its PCI DSS compliance in accordance with the SDP Program's 10.3.4 Implementation Schedule.

Note: All merchants must still maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation/reporting to Mastercard is a requirement. L3 merchants (Ecommerce merchants) are not eligible for the Risk-based Approach or PCI Compliance Validation Exemption Program.

2017 UPDATE:

[1] Level 1 and Level 2 Merchants located outside of the U.S. region may qualify as compliant with the Mastercard PCI DSS Risk-based Approach by validating compliance with the first two of six total milestones of the PCI DSS Prioritized Approach.

[2] Mastercard has expanded the qualification criteria for the Exemption Program as follows:

- Include Level 4 Merchants as eligible participants
- For a Level 1, Level 2, or Level 4 Merchant that does not have at least 75 percent of its annual total acquired Mastercard and Maestro transaction count processed through hybrid point-of-sale (POS) terminals, the merchant still will be qualified if it has implemented a validated point-to-point encryption (P2PE) solution listed on the PCI SSC website.

Q: How does a merchant qualify for the Mastercard Risk-based Approach?

To qualify for the Mastercard PCI DSS Risk-based Approach, a merchant must be a Level 1 or Level 2 Merchant located outside of the U.S. region and must satisfy all of the following:

- The merchant must certify that it is not storing Sensitive Card Authentication Data.
- On a continuous basis, the merchant must keep fully segregated the "Card-not-present" Transaction environment from the "face-to-face" Transaction environment. A face-to-face

Transaction requires the Card, the Cardholder, and the merchant to all be present together at the time and place of the Transaction.

- For a merchant located in the Europe Region, at least 95 percent of the merchant's annual total count of Card-present Mastercard and Maestro transactions must occur at Hybrid POS Terminals.
- For a merchant located in the Asia/Pacific Region, Canada Region, Latin America and the Caribbean Region, or Middle East/Africa Region, at least 75 percent of the merchant's annual total count of Card-present Mastercard and Maestro transactions must occur at Hybrid POS Terminals.
- The merchant must not have experienced an ADC Event within the last 12 months. At the discretion of Mastercard, this and other criteria may be waived if the Merchant validated full PCI DSS compliance at the time of the ADC Event or Potential ADC Event.
- The merchant must establish and annually test an ADC Event incident response plan.

A qualifying Level 1 or Level 2 Merchant may use the Mastercard Risk-based Approach by:

- Validating compliance with the first two of the six total milestones set forth in the *PCI DSS Prioritized Approach*
- Annually revalidates compliance with milestones one and two using an SAQ. The SAQ must be completed by internal staff trained and currently certified through the PCI SSC- offered ISA Program.

Q: How does a merchant qualify for the Mastercard PCI Compliance Validation Exemption Program?

To qualify for the Mastercard PCI Compliance Validation Exemption Program (the "Exemption Program"), which exempts the merchant from the requirement to annually validate its compliance with the PCI DSS, a merchant must be a Level 1, Level 2 or Level 4 Merchant and must satisfy all of the following:

1. The merchant validated its compliance with the PCI DSS within the previous twelve (12) months or, alternatively, has submitted to its acquirer, and the acquirer has submitted to Mastercard, a defined remediation plan satisfactory to Mastercard designed to ensure that the merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
2. The merchant does not store Sensitive Card Authentication Data. The acquirer must notify Mastercard through compliance validation reporting of the status of merchant storage of Sensitive Card Authentication Data;
3. The merchant has not been identified by Mastercard as having experienced an ADC Event during the prior twelve (12) months;
4. The merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements; and
5. The merchant has satisfied either of the following:

a. At least 75 percent of the merchant's annual total acquired Mastercard and Maestro Transaction count is processed through Hybrid POS Terminals, as determined based on the merchant's transactions processed during the previous twelve (12) months via the GCMS and/or Single Message System. Transactions that were not processed by Mastercard may be included in the annual acquired Transaction count if the data is readily available to Mastercard; **OR**

b. The merchant has implemented a point-to-point encryption (P2PE) solution listed on the PCI SSC website. *If a merchant has previously validated PCI DSS compliance with an onsite assessment to Mastercard and subsequently implements a PCI Council listed P2PE solution, the merchant will need to complete SAQ P2PE (using a QSA or ISA is not required) in order to qualify for the Exemption Program.*

An acquirer must retain all merchant certifications of eligibility for the Exemption Program for a minimum of five years. Upon request by Mastercard, the acquirer must provide a merchant's certification of eligibility for the Exemption Program and any documentation and/or other information applicable to such certification. An acquirer is responsible for ensuring that each Exemption Program certification is truthful and accurate.

How does an acquirer report merchants using the Risk-based Approach or participating in the PCI Compliance Validation Exemption Program?

The SDP Acquirer Submission and Compliance Status Form addresses PCI DSS compliance reporting for merchants validating compliance with the Risk-based Approach or participating in the PCI Compliance Validation Exemption Program.

- To report qualifying Level 1 or Level 2 Merchants using the Risk-based Approach, acquirers must complete the Risk-based Approach data fields located on the "Merchant Data" tab of the SDP Acquirer Submission and Compliance Status Form.
- To report qualifying Level 1, Level 2, or Level 4 Merchants participating in the PCI Compliance Validation Exemption Program, acquirers must complete the Exemption Program data fields located on the "PCI Validation Exemption" tab of the SDP Acquirer Submission and Compliance Status Form.
  - On an annual basis, the acquirer will complete the Exemption Program data fields on the "PCI Validation Exemption" tab via the SDP Acquirer Submission and Compliance Status Form attesting that the merchant continues to meet the Program's qualification criteria.

Q: I am a SDP Level 1 Service Provider. What are my PCI compliance validation requirements?

To validate compliance, a L1 Service Provider must successfully complete:

- An annual onsite assessment conducted by an appropriate PCI SSC approved Qualified Security Assessor (QSA)
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

2017 UPDATE

Mastercard recommends that a Level 1 Service Provider demonstrate to Mastercard their compliance with the PCI DSS Designated Entities Supplemental Validation (DESV) - appendix of the PCI DSS. An additional field (checkbox) has been added to *The Mastercard SDP Compliant Registered Service Provider List* to show those Service Providers that demonstrate compliance with the DESV.

Q: I am a SDP Level 2 Service Provider. What are my PCI compliance validation requirements?

To validate compliance, a L2 Service Provider must successfully complete:

- An annual self-assessment
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV)

2017 UPDATE

Mastercard recommends that a Level 2 Service Provider demonstrate to Mastercard their compliance with the PCI DSS Designated Entities Supplemental Validation (DESV) - appendix of the PCI DSS.

Q: Where can I find PCI compliance validation tools (for example, Self-Assessment Questionnaires (SAQs), Attestation of Compliance (AOCs), the Prioritized Approach Tool)?

The PCI Security Standards Council manages validation tools to assist merchants and Service Providers in demonstrating their compliance with the PCI Data Security Standard (PCI DSS). To view or download compliance validation tools and supporting documentation, visit the Document Library at www.pcisecuritystandards.org.

Q: What is Mastercard's ISA mandate?

The Mastercard ISA mandate applies to Level 1 and Level 2 Merchants:

- A Level 1 Merchant that uses an internal auditor for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the PCI DSS attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue to use an internal auditor.
- A Level 2 Merchant must ensure that staff engaged in self-assessing the merchant's compliance with the PCI DSS attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue the option of self-assessment for compliance validation.

Note: The Mastercard ISA mandate does not apply to L3 merchants.

Q: What is Mastercard's PA-DSS mandate?

All merchants and Service Providers that use third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS), as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the PCI PA-DSS Program Guide found in the Document Library at www.pcisecuritystandards.org.

2017 UPDATE

Mastercard recommends that a merchant (regardless of level) use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website to implement a payment application compliant with the PCI PA-DSS.

Q: What is Mastercard's SDP Program noncompliance assessment structure?

A merchant or Service Provider that is noncompliant with the SDP Program could be affected by potential SDP noncompliance assessments. 10.3.4 of the *Security Rules and Procedures Manual – Merchant Edition* addresses escalating assessments within a calendar year for both merchants and Service Providers if Mastercard requirements are not met.

Frequently Asked Questions – SDP Program Changes, 1 March 2017

Q: How has Mastercard revised acquirer SDP reporting requirements for merchants?

Mastercard will no longer require an acquirer to report merchant PCI DSS compliance to Mastercard on a quarterly basis. An acquirer will now submit the completed SDP Acquirer Submission and Compliance Status Form via e-mail to the SDP mailbox (sdp@mastercard.com) twice per year (semi-annually) on 31 March and 30 September.

Q: Why has Mastercard revised the qualification criteria for the Mastercard PCI DSS Risk-based Approach?

In the 2016 release of version 3.2 of the PCI DSS, certain requirements of milestones 3 and 4 of the *PCI DSS Prioritized Approach* were incorporated into milestones 1 and 2. As a result, Level 1 and Level 2 Merchants located outside of the U.S. region may qualify as compliant with the Mastercard PCI

DSS Risk-based Approach by validating compliance with the first two of six total milestones of the *PCI DSS Prioritized Approach* instead of the first four milestones.

Q: Why has Mastercard revised the qualification criteria for the Mastercard PCI Compliance Validation Exemption Program?

To provide increased flexibility in the Mastercard Standards and to further align with the industry, Mastercard has expanded the qualification criteria for the Mastercard PCI Compliance Validation Exemption Program to now include Level 4 Merchants as eligible participants and merchants that have implemented a validated point-to-point encryption (P2PE) solution listed on the PCI SSC website to qualify for the Exemption Program.

Note: SDP Level 3 Merchants are not eligible for the Exemption Program, as they are an e-commerce only merchant class; the Exemption Program is only applicable to card-present merchants.

Q: Why is Mastercard recommending that Level 1 and Level 2 Service Providers demonstrate compliance with the PCI DSS Designated Entities Supplemental Validation (DESV)?

In June 2015, the PCI SSC published the DESV – an appendix to the PCI DSS. The DESV appendix provides additional criteria for an entity to demonstrate that the entity's PCI DSS controls are effectively maintained to protect payment data from compromise. Because this appendix was specifically designed for entities that may be at greater risk for compromise, Mastercard is recommending that Level 1 and Level 2 Service Providers demonstrate compliance with the DESV. An additional field (checkbox) has been added to *The Mastercard SDP Compliant Registered Service Provider List* to show those Service Providers that demonstrate compliance with the DESV.

Q: Why has Mastercard revised compliance validation requirements for Level 3 and Level 4 Merchants to include the option of engaging a PCI SSC QSA for an onsite assessment?

According to SDP Program rules, Level 3 and Level 4 Merchants can validate PCI DSS compliance by successfully completing an annual PCI Self-Assessment Questionnaire (SAQ) and quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV). As a result of feedback received from acquirers and a number of Level 3 and Level 4 merchants requesting the option to have an annual onsite assessment conducted by a PCI SSC-approved QSA instead of completing an annual self-assessment, Level 3 and Level 4 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

Note: Option for Level 3 and Level 4 Merchants to validate PCI DSS compliance through an onsite assessment conducted by a QSA is not required.

Q: Why is Mastercard recommending that a merchant (regardless of level) use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website to implement a PA-DSS compliant payment application?

Because account data compromise investigations have shown that improper installation of a payment application can create opportunities for a merchant's network to be compromised, Mastercard is recommending that all merchants use a QIR – *PCI SSC trained professionals in the secure installation of PA-DSS validated payment applications into merchant environments* - listed on the PCI SSC website when implementing a PCI PA-DSS compliant payment application.

Q: Why is Mastercard requiring that acquirers have a risk management program in place for their Level 4 Merchants? When will it become effective and how will acquirers certify to Mastercard the status of their risk management program?

Although an acquirer is not required to validate the PCI DSS compliance status of its Level 4 Merchants to Mastercard, a Level 4 Merchant is still required to be PCI DSS compliant as per Mastercard Standards.

A number of acquirers already have a Level 4 Merchant risk management program in place to identify and address payment card security risk. For those acquirers who do not, Mastercard will require all acquirers to implement a Level 4 Merchant risk management program by 31 March 2019. Validation of Level 4 Merchant PCI DSS compliance to Mastercard via the SDP Acquirer Submission and Compliance Status Form will continue to remain optional; however, an additional - yes or no - question has been added to the SDP Acquirer Submission and Compliance Status Form for acquirers to attest to having a risk management program in place for their Level 4 Merchants.

Q: How will a Level 4 Merchant risk management program help acquirers manage risk to the payment system?

A Level 4 Merchant risk management program will allow acquirers to identify and manage security risk within their Level 4 Merchant portfolio. Using a risk-based approach for their Level 4 Merchants, acquirers are able to focus on merchants that represent the highest risk to the payment system. The Level 4 Merchant risk management program will be designed and managed by the acquirer in order to customize a program that fits their Level 4 Merchant portfolio.

Q: Will Mastercard offer guidance to help acquirers with their risk management programs?

Yes. Mastercard will offer guidance to help acquirers create and manage their risk management program. For more information on an acquirer's Level 4 Merchant risk management program, please send an email to sdp@mastercard.com.

Q: What is Mastercard's position on Corporate Cards and PCI compliance?

Corporate card clients are not required to provide validation that their corporate card data is protected in accordance with PCI DSS requirements (e.g. internal storage of corporate card information, such as travel profiles). This includes corporate cards used for multi-use (physical or virtual cards) and single-use virtual card numbers (SU-VCN). In addition, the corporate card client is not obligated to secure their data since the corporation assumes and holds the risks if cardholder data is compromised. However, Mastercard highly recommends that corporate card clients consider utilizing PCI DSS controls to protect their corporate card data. Entities should also consider adequately segmenting their own commercial card data from other consumer or merchant data in order to reduce the PCI DSS scope and risks of compromise.

Any system or entity besides the corporate card client that stores, process or transmits corporate card PANs (physical or virtual) must be PCI DSS Compliant.

Q: What is Mastercard's position on Single Use Virtual Card Numbers and PCI compliance?

Mastercard does not consider Single Use Virtual Card Numbers (SU-VCNs) to be in scope of PCI DSS requirements. The SU-VCN becomes inactive/disabled after only one authorization; therefore, the virtual PAN data cannot be reused for fraudulent activities within the payment ecosystem. However, it is important to note that even though a SU-VCN may be considered "out of scope" for PCI DSS, it does not mean that the systems and/or entities that are storing, transmitting or processing the SU-VCN are also out of scope. PCI DSS will apply anywhere a multi-use PAN is stored, transmitted or processed. If the systems storing, transmitting or processing the SU-VCN also store, transmit or process multi-use PANs, those systems will remain in scope of PCI DSS requirements.

Q. Should merchants only utilize approved PCI PTS devices?

Yes. Merchants implementing new payment devices are encouraged to review the Council's listing of PCI PTS-approved devices and their expiry dates. For more information on the usage and replacement of PTS devices, send an email to POI_security@mastercard.com.

Q: Are Terminal Servicers required to be PCI DSS compliant?

Yes. A Terminal Servicer that performs services involving the storage, transmission, or processing of account, cardholder, or transaction data must comply with the PCI DSS and is required to validate their compliance to Mastercard annually. A Terminal Servicer should also be registered as a Service Provider with the Mastercard Service Provider Registration Team (service_provider@mastercard.com).