FREQUENTLY ASKED QUESTIONS

The MasterCard Site Data Protection (SDP) Program

MERCHANTS

Can Level 1 merchants currently use internal auditors to perform an onsite assessment?
Yes. However, after June 30, 2012, the MasterCard SDP Program mandate for PCI DSS compliance validation will require Level 1 merchants to successfully complete an annual onsite assessment conducted by a PCI SSC certified QSA or an internal auditor who has attended and passed the PCI ISA training offered through the PCI SSC.

Will level 2 merchants be permitted to continue to validate with a Self Assessment Questionnaire indefinitely, provided they attend and pass the required PCI SSC ISA training?
Yes, Level 2 merchants will be permitted to continue to validate annually via a Self Assessment Questionnaire (SAQ) provided that the merchant's internal auditors have attended and passed the PCI ISA training offered through the PCI SSC prior to June 30, 2012. After the June 30, 2012 effective date, the ISA must perform the assessment and complete its SAQ.

Does the merchant's staff simply need to be trained and certified by June 30, 2012? Or does the merchant also need to revalidate its SAQ or onsite assessment by June 30, 2012 using its certified ISA?
The deadline is only specific to training and certification. Merchants should continue to validate compliance on an annual basis. There is no requirement to re-validate by June 30, 2012.

> ***Rules Language:***
> *Effective 30 June 2012, Level 2 merchants must ensure that staff engaged in the self-assessment attend the PCI SSC ISA Program and pass the associated accreditation examination annually to continue the option of self-assessment for compliance validation.*

If a merchant has a corporate structure that involves franchisees or subsidiaries, does the merchant need to send individuals from each franchisee or subsidiary to PCI SSC training, or can one corporate individual be PCI SSC trained and certified?
The rule is intended to provide flexibility for merchants. If there is one corporate employee that is accountable and has appropriate oversight into the applicable franchisees or subsidiaries, then that individual could perform assessments on behalf of the corporation.

Where can we find out more information on the ISA Program?
Please visit https://www.pcisecuritystandards.org/training/isa_training.php for more information and registration details.

How does MasterCard define an ISA?
An ISA is a merchant employee who has attended the PCI SSC ISA Program training and passed any associated accreditation on an annual basis.

How does the ISA Training requirement affect Level 3 merchants?
Level 3 merchant requirements remain unchanged. The initial PCI compliance validation date for Level 3 merchants was June 2005.

How does MasterCard define a QSA?
A Qualified Security Assessor (QSA) is a firm with employees individually qualified as PCI Security Standards Council (SSC) QSAs. The firm must be listed at https://www.pcisecuritystandards.org/approved_companies_providers/index.php.

When does the new MasterCard PA-DSS mandate go into effect?
The Payment Application Data Security Standard (PA-DSS) Program mandate is effective July 1, 2012. PA-DSS requires vendors of third party payment applications to ensure proper security controls are in place to safeguard cardholder data. Many of the controls within PA-DSS are designed to specifically address common vulnerabilities that were identified as main causes in credit card data loss. The MasterCard PA-DSS mandate will help continue to drive global adoption of and compliance with the PCI DSS for all stakeholders within the payment channels.

Effective 1 July 2012, MasterCard requires all merchants and Service Providers that use third party-provided payment applications to only use those 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 at www.pcisecuritystandards.org.

If a merchant has outsourced all their cardholder data processes and are currently using SAQ A to attest they are not storing, processing or transmitting data because they are using a PCI certified Third Party Processor (TPP), can they use SAQ A?
Due to the fact the merchant is attesting that it does not handle cardholder data and the TPP it is using requires an on-site assessment by a QSA for validation, the merchant can use SAQ A to validate compliance. Please note that does not apply to face to face merchants.

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.

Single Use Virtual Card Numbers

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.

ACQUIRERS

What is "*Initiated*"?

Initiated is when a merchant has started implementing the PCI DSS and has reported initial steps to their acquirer. The first step for a merchant is usually implementing PCI DSS requirement 11.2 by completing a quarterly scan with an Approved Scanning Vendor (ASV) and addressing any issues identified during the scan. Customers reporting via Prioritized Approach worksheet can report validation of requirements met within each milestone. This type of reporting is also considered an initiated step for non-compliant merchants. After initiating, the merchant must continue to demonstrate progress toward full PCI DSS compliance. Activities such as reading the standard, sending an RFP to potential vendors, and creating project plan, are not considered initiated as the goal is to mitigate risks to cardholder data as soon as possible.

If a merchant validates PCI compliance annually in the middle of the year, will the effective date be based on the calendar year, or one year from the date of merchant notification?

The compliance renewal date is one year from the date the merchant validates PCI compliance with their acquirer. However, the merchant should confirm with its individual acquirers to determine its exact validation dates.

If a merchant transitions or is reclassified from one merchant level to another (for example transitions from Level 4 to Level 3) due to the transaction volume increase, how long does the merchant have to validate compliance.

The acquirer must ensure, with respect to each merchant that transitions from one PCI level to another, that each merchant achieves and validates PCI compliance as soon as practical, but not later than one year after the date of the event that results in the merchant reclassification.

How long does a newly acquired merchant affected by the SDP mandate have to validate PCI compliance?

Any newly boarded Level 1, 2 or 3 merchant should have already met the initial PCI compliance validation dates. As MasterCard's Prioritized Approach reporting is required for all non-compliant merchants, a merchant that is non-compliant upon boarding is required to provide current compliance progress and status via the Prioritized Approach. At the next quarterly SDP report submission, the merchant's non-compliance status should be reported via the Prioritized Approach reporting fields. The Prioritized Approach helps acquirers and MasterCard determine the level of PCI DSS compliance activity completed by the merchant and helps measure the level of risk associated with noncompliance.

What does MasterCard require from the acquirer as validation?

PCI compliance information is reported to MasterCard on quarterly basis using the Acquirer Submission and Compliance Status Form. Please visit www.mastercard.com/sdp to download the Acquirer Submission and Compliance Status Form. Please note: MasterCard does not receive PCI validation documentation directly from merchants.

Does the Prioritized Approach replace the PCI DSS?

No. All businesses that touch payment card data are required to achieve and maintain compliance with the PCI DSS. The Prioritized Approach does not replace the standard.

Why is MasterCard requesting acquirers to report on merchant compliance using the Prioritized Approach?

The Prioritized Approach helps acquirers and MasterCard determine the level of PCI DSS compliance activity completed by the merchant and helps measure the level of risk associated with noncompliance.

As an Acquirer, how will I communicate progress against the Prioritized Approach to MasterCard?

Acquirers can use the information provided in the Prioritized Approach tool. This tool allows merchants and service providers to measure and track their progress to populate the SDP Acquirer Submission and Compliance Status Form.

Is the Prioritized Approach a fast track to PCI Compliance?

No. The Prioritized Approach will help organizations understand where they can act first on their compliance journey to have the most immediate impact on card data security. All requirements of the PCI DSS must be met and maintained in order to achieve compliance.

What entities do the six new Prioritized Approach reporting data fields in the MasterCard Acquirer Submission and Compliance Status Form pertain to?

These six new fields only apply to those merchants completing SAQ D or those merchants required to have onsite assessments. Entities that are reported as PCI compliant do not have to complete the Prioritized Approach fields.

How do acquiring banks fill out the PA-DSS compliance fields?

When completing the PA-DSS fields on the SDP Acquirer Submission and Compliance Status Form, use the drop-down menu to select from the following response options as to whether the merchant uses third party-provided payment applications that are PA-DSS compliant.

Response	Description
Yes	The merchant has validated that it is using an applicable payment application listed on the PCI SSC Web site.
No	The merchant is using a commercially available payment application not listed as PA-DSS compliant on the PCI SSC Web site.
Not Applicable (N/A)	The merchant is not using an applicable payment application. For example, the merchant is using a dumb terminal or custom application in conjunction with appropriate PCI DSS controls to protect cardholder data stored, processed, or transmitted by the terminal, payment application, or both.

Acquirers must complete the form in its entirety and submit via e-mail message to sdp@mastercard.com.

SERVICE PROVIDERS

What does MasterCard require from the acquirer as validation for their Service Providers?

This depends on what category of Service Provider they fall under with MasterCard. Note that MasterCard requires all newly identified Service Providers first register as an MSP (Member Service Provider) with the MSP registration team at MasterCard. The MSP team can be contacted via member_service_provider@mastercard.com.

Please Note: that one or more member banks can enter a service provider into the system. If a Service Provider has a direct relationship with one or more of our member banks, the Service Provider should contact each one for separate registration. If the Service Provider does not have a direct relationship with one or more of our members, it would need to get sponsorship from their customer's bank to get set up (this may be either a merchant or another processor, such as a Third Party Processor – many of which have direct relationships with our banks).

Once a Service Provider is registered with MasterCard, it is required to validate PCI compliance. All TPPs (regardless of volume) and DSEs with > than 300,000 transactions annually are required to successfully complete an onsite assessment and quarterly network scans. Validation in the form of the Attestation of Compliance (or Certificate of Validation) is submitted only once annually to satisfy the SDP requirement. The AOC for onsite assessments must be completed by the QSA and should be submitted by the QSA to MasterCard at PCIReports@mastercard.com.

For those DSEs performing < 300,000 transactions annually, MasterCard accepts the "AOC for Self-Assessment Questionnaire D – Service Provider Version 1.2" and the most recent clean scan report.

How can a Service Provider be listed on the Compliant Service Provider List on the SDP website?
MasterCard only lists those Service Providers that have successfully completed an annual onsite assessment performed by a QSA and provided validation to MasterCard.

Where can a Service Provider find the latest version of the Service Provider PCI Action Plan?
Please go to www.mastercard.com/sdp or email sdp@mastercard.com to request the latest version.

Where can I find the Attestation of Compliance (AOC) form?
Please visit www.pcisecuritystandards.org to find the current AOC forms.