

# Site Data Protection

Payment System Integrity



## FAQs

### Site Data Protection Program Changes

---

#### Summary

MasterCard has revised the MasterCard Site Data Protection (SDP) Program to help ensure member, merchant, Third Party Processor (TPP), and Data Storage Entity (DSE) compliance with the Payment Card Industry Data Security Standard (PCI DSS). The SDP Program revisions include:

- Changes to the SDP noncompliance assessment structure
- A new requirement for Level 1 and Level 2 merchants to use a PCI Security Standards Council (SSC) certified Qualified Security Assessor (QSA) for the mandatory annual onsite assessment
- The reclassification of Level 1 Service Providers to include TPPs (regardless of volume) and DSEs with greater than 300,000 transactions annually
- The reclassification of Level 2 Service Providers to DSEs with 300,000 or less transactions annually
- Reporting using the Prioritized Approach

#### Merchants

**All Level 1 merchants must now use a PCI SSC certified QSA to conduct an onsite assessment and then validate compliance. Is this effective immediately?**

All Level 1 merchants that have engaged an internal auditor before 15 June 2009 must validate compliance with the PCI DSS via an annual onsite assessment conducted by a PCI SSC certified QSA by 31 December 2010.

**Is it accurate that MasterCard will require Level 2 merchants to conduct annual on-site reviews of their security controls by third party QSAs.**

MasterCard announced revised requirements for Level 2 merchants to use a Qualified Security Assessor (QSA) to complete a mandatory annual onsite data security assessment by December 31, 2010.

**If so, when was the change made and why?**

These changes were announced in the MasterCard *Global Security Bulletin* No. 6 published on June 15, 2009 and distributed directly to MasterCard acquirers and processors. The current enhancement of validation requirements for PCI compliance provides for independent third party review to facilitate to consistent application and implementation of DSS requirements.

# Site Data Protection

Payment System Integrity



## **All Level 2 merchants must now use a PCI SSC certified QSA to conduct an onsite assessment and then validate compliance. Is this effective immediately?**

Effective 31 December 2010, all Level 2 merchants must complete an annual onsite assessment conducted by a PCI SSC certified QSA. For now, Level 2 merchants may validate PCI compliance via the Self Assessment Questionnaire (SAQ). However by 31 December 2010, Level 2 merchants **must** validate compliance via an annual onsite assessment.

## **What steps does MasterCard suggest that Level 1 and Level 2 merchants take to complete an onsite assessment prior to the December 31st, 2010 mandate?**

To fulfill this requirement by the 31 December 2010 deadline, MasterCard strongly encourages that all Level 1 and Level 2 merchants engage a PCI SSC certified QSA immediately.

## **How do the changes to the Site Data Protection Program affect Level 3 merchants?**

Level 3 merchant requirements remain unchanged. The PCI compliance 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/qa\\_asv/find\\_one.shtml](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml)

## **Can merchants use their employees to perform onsite assessments who are certified QSAs?**

The PCI Security Standards Councils only certifies QSAs who work for a qualified organization that has been vetted and approved to operate as a QSA firm. Companies must use a PCI SSC certified QSA to perform an annual onsite assessment. QSA have met yearly training requirements and are validated via a quality assurance program administered by the PSI SSC. PCI SSC QSA firms are listed [here](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml). ([https://www.pcisecuritystandards.org/qa\\_asv/find\\_one.shtml](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml))

## **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 the 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 new SDP mandate have to validate PCI compliance?**

PCI compliance dates have passed and merchants are required to be PCI compliant upon boarding. As a best practice, acquirers should board merchants that are PCI compliant. This process prevents merchants from switching acquirers to avoid having to become PCI compliant.

# Site Data Protection

Payment System Integrity



## **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. Once a merchant is PCI compliant, the merchant must be registered by the acquirer in the MasterCard Registration Program (MRP). The merchant is then considered SDP compliant. Please visit [www.mastercard.com/sdp](http://www.mastercard.com/sdp) to find the Acquirer Submission and Compliance Status Form. Please note: MasterCard does not receive the validation documentation directly from merchants.

## **If a Level 2 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), do they need to do an on-site assessment now versus SAQ A?**

Due to the fact the Level 2 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 Level 2 merchant can still use SAQ A to validate compliance.

## **Does the Prioritized Approach replace the PCI DSS 1.2?**

No. All businesses that touch payment card data are required to achieve and maintain compliance with the PCI DSS 1.2. 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 in which merchants and service providers measure and track their progress to populate the revised Acquirer Submission and Compliance Status Form (V3.1).

## **Is this 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 1.2 must be met and maintained in order to achieve compliance.

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

These six new fields only apply to those merchants using SAQ Type D and those merchants receiving onsite assessments

# Site Data Protection

Payment System Integrity



## Service Providers

### **How do the recent SDP Program changes affect Service Providers?**

DSEs with greater than 300,000 annual transactions are now considered Level 1 Service Providers.

### **What does MasterCard require from the acquirer as validation, copy of AOC, SAQ or copy of network scan?**

MasterCard requires that all newly identified Service Providers must 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](mailto:member_service_provider@mastercard.com).

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 they do not have a direct relationship with one or more of our members, they 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, they are 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 to [PCIReports@mastercard.com](mailto:PCIReports@mastercard.com). 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](mailto: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.

Please note that as of January 1, 2009, MasterCard will no longer list those Service Providers who have only submitted an SAQ. The posting will contain only those entities that have successfully completed an annual onsite review.

### **How can a Service Provider be listed on the Compliant Service Provider List on the SDP website?**

As of January 1, 2009, MasterCard will no longer list those Service Providers who have only submitted an SAQ. The posting will contain only those entities that have successfully completed an annual onsite assessment and provided validation to MasterCard.

### **Where can a Service Provider find the latest version of the Service Provider PCI Action Plan?**

Please email [sdp@mastercard.com](mailto:sdp@mastercard.com) and request the latest version.

### **Where can I find the Attestation of Compliance form?**

Please visit [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) to find the new AOC.