

PCI Data Security Standard Validation for Service Providers

Prepared by NC Office of the State Controller

December 1, 2008

Merchants that use a “service provider” to process, store, and/or transmit their card transactions are required by the PCI Data Security Standard (PCI DSS) to ensure that the service provider is compliant with the PCI DSS. The primary requirements that apply are found in section 12.8 of the PCI DSS. A “service provider” would include, but not be limited to, any company providing a gateway service, a data storage service, or a web hosting service.

	PCI DSS Requirement	Testing Procedure
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	If the entity being assessed shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:
12.8.1	Maintain a list of service providers.	Verify that a list of service providers is maintained.
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status.	Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.

A merchant is required to manage each service provider by: 1) maintaining a written agreement (between the merchant and the service provider) that includes an acknowledgement that the service provider is responsible for the security of cardholder data, that is either processed, stored, and/or transmitted; and 2) maintaining a program to monitor the service provider’s compliance status.

There are several methods that could be deployed to validate the service provider’s compliance, and the method deployed depends upon the merchant’s risk assessment of the service being provided. The different methods of validation that the merchant could require of the service provider in a written agreement (to fulfill requirement 12.8.2) include:

- 1) The service provider to obtain and provide the merchant evidence of a Report on Compliance (ROC) prepared by a Qualified Security Assessor (QSA), and to undergo quarterly vulnerability scans; or
- 2) The service provider to take the same steps that a merchant would be expected to take, i.e., prepare and provide to the merchant version D of the annual Self-Assessment Questionnaire (SAQ), and to undergo quarterly vulnerability scans.

The current version of the PCI DSS does not specify how a service provider is to provide evidence to the merchant that it has been validated as being PCI DSS compliant, other than requiring a written agreement between the merchant and the service provider, and requiring a monitoring of the

compliance status by the merchant. However, Visa's Cardholder's Information Security Program (CISP) does specify requirements for "service providers" to become validated by February 1, 2009, depending upon the level of the service provider. According to Visa, a service provider that processes more than 300,000 transactions per year is considered a "Level 1" service provider and is required to undergo an onsite security assessment by a QSA. A service provider that processes less than 300,000 transactions per year is considered a "Level 2" service provider and is not required to undergo an onsite security assessment by a QSA. The Visa's CISP requirements for service providers are found at: http://usa.visa.com/merchants/risk_management/cisp_service_providers.html. While MasterCard considers a Level 1 service provider to be one that processes over 1 million transactions per year, the more restrictive requirement of the two card brands that are accepted by the merchant should be adhered to. See MasterCard's site: <http://www.mastercard.com/us/sdp/serviceproviders/index.html>

The different methods of monitoring a service provider's compliance status by the merchant (to fulfill the requirement of 12.8.4) could include, depending upon the written agreement between the merchant and the service provider, and depending upon whether the service provider is a Level 1 or Level 2 service provider:

- 1) For service providers required to undergo an onsite security assessment by a QSA - The merchant should obtain from the service provider a copy of the Report on Compliance (ROC) prepared by the QSA, or attestation that a current ROC has been issued. In addition to having obtained a ROC from a QSA, some service providers, but not all, have registered to be included on Visa's List of Compliant Service Providers, which may be viewed at Visa's website.
- 2) For service providers **not** required to undergo an onsite security assessment by a QSA - The service provider should engage the services of a Qualified Scanning Vendor (QSV) to provide an ongoing remote validation service (annual SAQ-version D and quarterly vulnerability scans), and provide the merchant with the results of the SAQ and scans, as may be requested. In certain cases (e.g., web hosting company that only hosts the website for the merchant), the merchant may be permitted to enroll the service provider (hosted website) in the remote validation service being offered by the Office of the State Controller (TrustKeeper), which allows the merchant and SunTrust Merchant Services to view the results of the SAQ and the scans.

For those merchants that have an existing contract, and the existing contract does not sufficiently satisfy requirement 12.8.2, requiring a "written agreement" addressing the PCI data security responsibilities of the service provider, OSC has a "[Sample Addendum for Requirement 12.8](#)" available on its website.

For those merchants that are acquiring the services of a service provider for the first time, or in the case of renewing services currently being provided, requirement 12.8.3 applies. Prior to engagement of services, the merchant must ensure that due diligence is in place to ensure compliance with the PCI DSS.