PCI Data Security Standard Validation for Service Providers

Prepared by South Carolina Office of the State Treasurer

Revised February 13, 2020

Service Providers Subject to PCI Data Security Standard

An agency using a service provider to store, process, or transmit cardholder data on an agency's behalf is required to ensure that the service provider is compliant with the "Payment Card Industry Data Security Standard" (PCI-DSS). The PCI Security Council's definition of a "service provider" is a "*Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.*"

Two Types of Service Providers

A service provider is any entity that processes or transmits cardholder data on the agency's behalf, such as a payment gateway. The entity is normally a "third-party" service provider with which the agency contracts. South Carolina Interactive LLC (SCI) that provides web portal services to agencies in South Carolina is an example of a third-party "payment gateway" service provider. Examples of other service providers include Touchnet as an offeror of its PayPath Gateway used by universities; and SunTrust Merchant Services as an offeror of its payment gateways (PayPoint, Payezzy, CardConnect).

A service provider can also be an entity that provides web hosting services and/or manages components of the agency's cardholder data environment (CDE), such as routers, firewalls, databases, physical security, and/or servers. This could be a third-party service provider. However, in the government arena, a separate agency within the government that that provides IT-related services to multiple agencies could be considered a service provider. Such an entity is referred to as an "internal" service provider. In some cases, the SC Department of Administration's Division of Technology Operations (DTO) could be considered an internal service provider.

PCI Requirements for Service Providers

The primary requirements pertaining to service providers from an agency's perspective are found in sections 12.8, 12.9, and 12.11 of the PCI-DSS.

	PCI DSS Requirement (Version 3.3)
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
12.8.1	Maintain a list of service providers including a description of the service provided.
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 or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise

	stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
12.11	**Additional requirement for service providers only:** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes Note: This requirement was a best practice until January 31, 2018, after which it became a requirement.

A merchant is required to <u>manage</u> each service provider by:
1) Maintaining a <u>written agreement</u> (between the merchant and the service provider) that includes an acknowledgement that the service provider is responsible for the security of cardholder data the service provider possess or otherwise stores, processes or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment; and

2) Maintaining a program to <u>monitor</u> the service provider's compliance status on at least an annual basis.

There are several methods that could be employed to verify a service provider's PCI compliance. The method would depend upon the agency's risk assessment of the service being provided, and whether the service provider is a third-party or an internal service provider. Verification could include either:
1) Require the service provider to obtain and provide the agency evidence of a "Report on Compliance" (ROC) prepared by a Qualified Security Assessor (QSA)

2) Verify that the service provider is listed on either Visa's or MasterCard's list of approved service providers:
    • https://www.visa.com/splisting/searchGrsp.do
    • https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
    (Note that an internal service provider would not be on either list.)

3) Require the service provider to take the same steps that a merchant would be expected to take to validate its compliance (i.e., prepare version D of the annual Self-Assessment Questionnaire (SAQ), and to undergo quarterly external vulnerability scans), and provide evidence of validation of compliance as may be requested.

Two Levels of Service Providers
According to Visa's Cardholder's Information Security Program (CISP), there are two levels of service providers. A service provider that processes more than 300,000 transactions per year is considered a "Level 1" service provider and is <u>required</u> 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 <u>not</u> required to undergo an onsite security assessment by a QSA. 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 (Visa's) should be adhered to.

The card brands' requirements for service providers can be viewed at:
- Visa - http://usa.visa.com/merchants/risk_management/cisp_service_providers.html.
- MasterCard - http://www.mastercard.com/us/sdp/serviceproviders/index.html

Two Arrangements with Service Providers

An agency may utilize a service provider to process merchant card transactions under one of two types of arrangements:
1) Agency is considered the "merchant of record (MOR);" or
2) Service provider is considered the "merchant of record (MOR)"

The agency's arrangement with the service provider determines the degree of applicability (scope) to the PCI Data Security Standard (PCI-DSS).

Previously, SC.Gov, the portal provided by SC Interactive (SCI), has offered both types of arrangements. However, SCI now only offers the option where the agency is the MOR. Plans are for those entities that currently acquire services where SCI is the MOR will undergo a conversion process where the agency is the MOR. An agency subscribing to services offered by SCI, or any other service provider, should be aware of the arrangement being utilized. The two arrangements are discussed below.

Service Provider as Merchant of Record (MOR)

Under arrangements where the service provider is considered the MOR, card transactions are processed under the service provider's merchant number it has with its merchant card processor (e.g., Fiserv's STMS, Elavon, etc.). The agency is not issued a merchant number, but perhaps an account number assigned by the service provider. Such service provider must be registered with the card brands as a "payment facilitator."

The PCI-DSS implications for the agency are greatly reduced, but not eliminated entirely. Under such arrangements, the service provider, not the agency, is directly accountable to the merchant card processor for all requirements of the PCI-DSS. The agency is responsible for certain requirements of the PCI-DSS, at least requirements 12.8 and 12.9.

However, as indicated in requirement 12.8.2, the agreement with the service provider may include terms that require the agency to be compliant with the PCI-DSS as well. It is advisable for the requirements assigned to the agency be identified in writing. Such terms in the agreement may have the effect of passing liabilities associated with a security breach along to the agency, if the agency's non-compliance contributes to the breach. The agency may therefore be accountable to the service provider for compliance, not to the merchant card processor.

For agencies using SC Interactive (SCI) under the arrangement where SCI is the MOR, the follow terms in SCI's agreements are examples of where the service provider passes on certain liabilities for PCI-DSS compliance to the agency.

Compliance with the Payment Card Industry's Data Security Standards
During the terms of this Agreement, the parties agree to be compliant with the applicable portions of the Payment Card Industry's Data Security Standards (the "PCI DSS"), as amended from time to time. Upon request, a party agrees to provide the other party (in this case, also a requesting party) with written proof of its compliance with the PCI DSS.

PCI-DSS Compliance
The parties understand and agree to comply with the Payment Card Industry Data Security Standard ("PCI DSS") and any amendments thereto. The parties acknowledge that each party is responsible for securing cardholder data that it may transmit, store, or process on its systems. The parties agree to maintain a list of which PCI DSS requirements are managed by SCI, and which requirements are the responsibility of Agency to include in Agency's PCI DSS reviews. Upon request, a party agrees to provide the other party (in this case, also a requesting party) with written proof of its compliance with the PCI DSS. As the operator of the Swipe Device, Agency shall be responsible for compliance with PCI DSS version 3.0 and any current versions regarding the Swipe Devices, including, but not limited to, the safeguarding, maintenance, inspection and training obligations set forth in PCI DSS Requirement 9.9.

When the service provider is the MOR, any PCI-DSS validation required of the agency would be made to the service provider, not to the service provider's merchant card processor.

Agency as Merchant of Record (MOR)
Under arrangements where the agency is considered the MOR, card transactions are processed by the service provider, but under a merchant number assigned to the agency by the agency's merchant card processor (e.g., STMS). In addition, the agency may or may not be assigned an account number by the service provider.

Under such arrangements, the agency is accountable directly to the merchant card processor for all requirements of the PCI-DSS.   Requirements 12.8 and 12.9 regarding written agreements and monitoring the service provider's compliance is critical. Any fines levied by the merchant card processor would be levied against the agency, not against the service provider.

Attesting PCI Data Security Compliance

The State Treasurer issued a PCI Data Security Compliance Policy in July 2016, requiring all participants to adhere to the PCI Data Security Standard (PCI-DSS). A supplemental policy was issued in February 2020 specifying the participant's required process for attesting PCI compliance, as well specifying STO's process for assisting STMS in the monitoring process. The supplemental policy specifies timeframes required to comply and remediation requirements in case of non-compliance.
The policies, as well as a PCI Compliance Roadmap document, can be viewed at the Treasurer's website:
https://treasurer.sc.gov/government/banking/

Normally, an agency only has one primary merchant ID (MID) under which it should attest its compliance. If an agency uses SCI as its processor in addition to using STMS directly, it will be assigned two primary MIDs, one for each processor. In such case the agency must complete two PCI attestations (SAQs), one for each primary MID. This is because the MID associated with SCI is grouped under a different Corp MID than the one associated with STMS.

Comparison of PCI Data Security Standard (PCI-DSS) Requirements Agency Using STMS as Primary Processor Versus Using SCI (SC.Gov) as Primary Processor			
Primary Processor:	**STMS – Statewide Contract**	**SC Interactive's (SCI) SC.Gov (aka NIC-USA)**	
	Agency is Merchant of Record (MOR)	**If SCI is MOR**	**If Agency is MOR**
Agency's contract agreement with processor:	Participation Agreement (PA) with STMS	Statement of Work (SOW) with SCI	PA with STMS and SOW with SCI
Merchant number assigned?	FD assigns merchant number to agency	All agencies use same SCI's merchant number with FD	FD assigns merchant number to agency
Agency PCI compliance required?	Yes, per PA with STMS	Yes, per SCI's SOW	Yes, per STMS's PA and SCI's SOW
Validation of compliance required by agency?	Yes, via PCI Rapid Comply	Yes, as may be requested by SCI	Yes, via PCI Rapid Comply
Enrollment in STMS's PCI Rapid Comply to attest compliance?	Yes. For SAQ & scanning, or SAQ only.	PCI Rapid Comply not available to agency, since merchant number belongs to SCI, and no PA with STMS. Attest directly to SCI.	Yes. For SAQ & scanning, or SAQ only.
Agency required to subscribe to External Vulnerability Scanning?	Yes, if capture solution involves external-facing IP addresses belonging to an agency-owned server (PCI Rapid Comply is available for this service; Some universities use an ASV.)	Not for any SCI-owned servers. If SCI's Virtual Terminal feature is utilized, then agency's server may be subject to scanning, if external-facing IPs involved	Not for any SCI-owned servers. If SCI's Virtual Terminal feature is utilized, then agency's (merchant's) server should be scanned
Agency required to monitor SCI for PCI compliance?	N/A	Yes, Requirements 12.8 & 12.9	Yes, Requirements 12.8 & 12.9
SCI required to by listed as an approved service provider on card brands' websites?	N/A	Yes (NIC-USA)	Yes (NIC-USA)
PCI SAQs Required by agency?	Yes, within 90 days and annually thereafter.	Yes, in order to demonstrate compliance directly to SCI if requested; In paper format	Yes, within 90 days and annually thereafter.
Three requirements applying to all arrangements:	PCI Policy (Req. 12.1), PCI Security Incident Plan (Req. 12.10), PCI Employee Awareness Training Program (Req. 12.6). (Sample templates are available from STO.)		
Requirements applying to all if POS terminals are used	Device protection and tampering (Requirement 9.9)		
PCI Oversight Committee	Best practice. (Sample charter available from STO.)		
PCI Point of Contact	Required per STO's Supplemental PCI Compliance Policy.		