THE HONORABLE CURTIS M. LOFTIS, JR.
State Treasurer

SUPPLEMENTAL POLICY
Compliance with PCI Data Security Standard
Monitoring and Remediation Process
February 1, 2020

Purpose

On July 1, 2016, the State Treasurer's Office (STO) issued a policy entitled, "Compliance with PCI Data Security Standard." The general policy states in part:

> *"As a prerequisite for participating in the statewide merchant card services agreement provided by the State Treasurer's Office, each participant must execute a participation agreement, which among other things, obligates the participant to comply with the PCI Data Security Standard (PCI DSS). Each participant must subscribe to the appropriate services that allows for the validation of PCI compliance."*

The policy in its entirety can be viewed at: https://www.treasurer.sc.gov/media/52852/Compliance-with-PCI-Data-Security-Standard-July-2016.pdf

This supplemental policy is intended to provide uniform guidance and requirements regarding how STO will assist the merchant card services processor [i.e., SunTrust Merchant Services (STMS)] in its role of monitoring each participant's compliance with the Standard. A participant is a public procurement unit, as defined in S.C. Code Ann. § 11-35-4610(5) who desires to subscribe to services available under the Merchant Card Services Agreement. The monitoring process is designed to ensure that:

- Each participant's compliance status is appropriately tracked;
- Any required remediation action is performed on a timely basis; and
- The participant is provided sufficient opportunity to rectify any non-compliance status before services may be suspended by STMS, as provided for in the Merchant Card Services Agreement

Supplemental Policy: To accommodate the general policy's requirement to subscribe to a PCI Compliance Validation Service (CVS), and to allow uniform tracking of all participants' compliance status, each participant must be enrolled in STMS's "PCI Rapid Comply® Portal." The Participant can either report its compliance status using the portal's online attestation tool or request STMS to report the status on its behalf. STMS shall keep STO informed of the current status of all participants as reported. Any status of non-compliance will be subject to the rectification actions specified in this supplemental policy.

Point of Contact Assignment

Each participant must have a designated PCI point of contact (POC). The POC may be a staff person from either the Finance Office or the Information Technology Department. In either case, there must be coordination between the staff of both offices.

PCI Rapid Comply Enrollment

The POC must ensure that the participant is properly enrolled in the PCI Rapid Comply Portal. This includes being set up for the proper validation option: 1) SAQ only; or 2) SAQ and vulnerability scanning. An SAQ is a Self-Assessment Questionnaire.

New participants in the statewide contract must be enrolled in the portal before STMS will allow any assigned merchant IDs to be activated. Three basic requirements of PCI compliance must be completed before STO will sign off on the execution of a new Participation Agreement:

- Development of a PCI Data Security Policy
- Development of a Security Incident Plan
- Participation in an Employee PCI Awareness Training Program

In accordance with the Standard, new participants will be given a 90-day grace period after enrollment to attest its compliance status by submitting the appropriate SAQ through PCI Rapid Comply.

Some participants utilize a qualified security assessor (QSA) to assist in their validation process. QSAs normally use one of two methods in this process. They either:

- Assist the POC in submitting the SAQ through the online attestation tool; or
- Prepare an "Attestation of Compliance" (AOC) without using the tool and submit to STMS

In case of the latter, the participant must request STMS to report its compliance status through the PCI Rapid Comply portal on its behalf. This allows for the necessary tracking by both STMS and STO.

Compliance Status

While a merchant's PCI status is either compliant or non-compliant, there are certain degrees of any non-compliance status situation that may exist. The degree of non-compliance would indicate the level of risk associated with the non-compliance status.

The participant's overall non-compliant status could be the result of an isolated situation. For example, deficiency associated with only one merchant number or one capture method could be causing the overall non-compliance status. Regardless of the degree of non-compliance, the participant should document the cause of the non-compliance, assess the risk associated with the non-compliance, and take the appropriate remediation actions.

Participant's Management Monitoring

Each participant must implement a process whereby the designated POC keeps the entity's management abreast of any change in its PCI compliance status. Management should take the appropriate action to ascertain the actions necessary to remediate the non-compliance status.

STO Monitoring

STO will have access to reporting available through the PCI Rapid Comply portal indicating the status of each enrolled participant. For participants indicated as non-compliant, a preliminary high-level assessment will be made to determine if the status is due to a SAQ issue, a vulnerability scan issue, or both. Each non-compliant participant will be categorized as below.

- Non-Compliant – Newly noted, requiring a courtesy inquiry of the POC
- Non-Compliant – Issues known to be in the process of being addressed
- Non-Compliant – Ongoing issues dictating the completion of a written Remediation Action Plan

Notification of Non-compliance Status

Once a participant is aware of its non-compliance status (self-determined or otherwise), a determination must be made of the anticipated length of the non-compliance status. If the status is anticipated to last for an extended period (i.e., 30 days or more), the participant must notify STO of the discovered status.

Written Remediation Action Plan

A written Remediation Action Plan is required whenever it is anticipated that a non-compliant status will last longer than 60 days after the date the participant becomes aware of the status. The Plan should be submitted to STO within 30 days of the date the participant becomes aware of the status.

The Plan should include at a minimum the following:

- MID(s) affected
- Reason for the non-compliant status
- Assessment of degree of risk
- Actions to be taken to remediate the situation
- Anticipated time to complete the actions

STO's Monitoring of Remediation Action Plan

Once a Remediation Action Plan is submitted, the participant must provide STO with a monthly progress report until the remediation is completed. Based on the complexity of the remediation actions required and the length of time required, STO will involve STMS in the process. STO's monitoring process does not preclude STMS from requiring certain actions of the participant.

Involvement of Qualified Security Assessor (QSA)

Depending upon the nature of a non-compliance issue and the ability and expertise of the participant's staff to resolve the non-compliance issue, involvement of a Qualified Security Assessor (QSA) may be necessary to assist in the matter.

Extended Non-compliance Status

Should a non-compliance status exist for an extended period, resolution will depend upon the severity of the condition. If the condition exists longer than 90 days, STO will consult with STMS regarding appropriate follow-up actions.

STMS will consider the requirements of its compliance department and that of the card brands. STMS may elect to request extensions from the card brands on behalf of the participant if appropriate. Extensions granted by either STMS or the card brands may or may not involve fines.

Ramifications of Failure to Become Compliant

Failure of a participant to adhere to any of the requirements of this policy, including failure to remediate a non-compliant status may result in STMS suspending or terminating services, as provided for under Paragraphs 21, 25, and 26 of the "Bank Card Addendum to Master Services Agreement."

Approval of Policy Implementation

Curtis M. Loftis, Jr. South Carolina State Treasurer