Validation of PCI Compliance Requirements
NC Office of the State Controller
June 23, 2015

Purpose

The purpose of this document is to provide instructions to entities that subscribe to merchant cards processing services under the Master Services Agreement (MSA) the State of North Carolina has with SunTrust Merchant Services, LLC (STMS), dated February 1, 2015, regarding the process to "attest" their validation of compliance with the PCI Data Security Standard (PCI DSS).

Requirements

Master Services Agreement (MSA) Requirement - The MSA states that, "The vendor and participant shall comply with all Payment Card Industry (PCI) security standards." There are various requirements that must be adhered to, most which are contained in standards promulgated by the PCI Security Standards Council. The website for the Council is: https://www.pcisecuritystandards.org

Office of the State Controller (OSC) Policy - OSC's policy entitled, "Security and Privacy of Data," requires each participant in the MSA to: "Participate in any security assessments and security scans required by the associations and/or OSC, in order to be and to remain compliant with Payment Card Industry (PCI) Security Standards, and be responsible for any fines levied as the result of not being compliant." The policy can be viewed at the following link:
http://www.osc.nc.gov/policy/EC/500.13_Security_and_Privacy_of_Data.pdf

Components of PCI Requirements

There are three components of requirements pertaining to PCI:

1) Compliance
2) Validation
3) Attestation

Compliance is performed by the participant implementing infrastructure and procedures.

Validation of compliance is two-fold – 1) Pass a vulnerability scan at least quarterly; and 2) Complete annually a Self-Assessment Questionnaire (SAQ) with no exceptions. Validation of a successful scan must be performed by a "qualified scanning vendor" (QSV) (e.g., Coalfire). Validation of the completion of the SAQ can be performed either through a "qualified security assessor" (QSA) or by the participant itself.

Attestation of validation of compliance is required to be made by the participant (merchant). The frequency of attestation and the method of attestation depend upon the Level assigned to the participant (Levels 1, 2, 3, 4). The attestation of validation of compliance may be requested by the merchant card processor (STMS) periodically, dependent upon requests that it may receive from the card associations (i.e., Visa, MasterCard, American Express, Discover). The requests could apply to only certain Level merchants, or to all merchants.

Summary of Responsibilities

- **Participant**
  - Become compliant and remain compliant with the PCI Data Security Standard
  - Validate its compliance with the PCI Data Security
    Standard ƒ Quarterly for vulnerability scanning ƒ
    Annually for Self-Assessment Questionnaires (SAQs)
  - Attest its validation of compliance with the PCI Data Security Standard (As may be requested from time to time by STMS and/or the card associations)

- **SunTrust Merchant Services**
  - Ensure that all merchants (participants) comply with the PCI Data Security Standard
  - Provide attestation of validation of participants' compliance as may be requested from time-to-time to the card associations
  - Address any non-compliance issues with the participant

- **Office of the State Controller**
  - Provide participants requiring vulnerability scanning services through a Qualified Scanning Vendor (QSV) – Scanning to be performed monthly.
  - Provide participants with a tool to validate their compliance through a Qualified Security Assessor (QSA), and to attest such validation. Self-Assessment Questionnaire to be completed annually through an online portal.
  - Provide STMS with status reports indicating the attestation of validation made by the participants, as may be requested from time to time by STMS
  - Provide appropriate central oversight agencies (i.e., UNC General Administration, NC Community College System, and Local Government Commission) with periodic compliance status reports.

Two Categories of Participants
There are two categories of participants:

1) Those that require monthly vulnerability scanning of their Web facing IP addresses, <u>and</u> completion of an Annual Self-Assessment Questionnaire (SAQ)
2) Those that require completion of an Annual Self-Assessment Questionnaire (SAQ) <u>only</u>

Required Enrollment in Coalfire Portal Tool
OSC has contracted with Coalfire to provide participants in the Statewide MSA with an online portal tool, allowing all participants to: 1) perform their validation of compliance with the PCI DSS; and 2) attest such validation to STMS. The tool is called Navis Portal.

Effective December 2014, all participants are required to enroll in Coalfire, even if scanning services are not required. Enrollment will provide each participant the ability to complete the Self-Assessment Questionnaire (SAQ) that is required by the PCI DSS to be completed on an annual basis. Enrollment in Coalfire allows the SAQ to be completed online, instead of being completed in a paper format. It also facilitates the passing of the attestation information along to STMS, whenever STMS may require it.

Enrollment Level in Coalfire

Enrollment at the chain level provides several advantages:

- In some cases, there will be a decrease in the number of monthly scans. Currently, if a Web facing IP address is associated with multiple merchant numbers, that single IP address is scanned multiple times. Under enrollment at the single chain level concept, the single IP address will only be scanned once per month.
- In some cases there will be a decrease in the number of Self-Assessment Questionnaires (SAQs) that will have to be completed annually. Currently, multiple SAQs have to be completed, even if the associated multiple merchant numbers are performed under the same processing operation.
- Reporting of the attestation of validation of compliance to STMS will be for the entire agency, which is more in line with the "Doing Business As" (DBA) requirements of the card associations.
- In some cases, the process of attesting the participant's validation of compliance will be reduced to only once per year. Currently, multiple outlets may have anniversary dates that are spread throughout the year. While "compliance" is a continuing process, "validation" is only periodically (quarterly for scanning, and annually for SAQs).

Exceptions to Enrollment at the Chain Level

There may be some situations where it may be more appropriate for a participant (entity) to have multiple enrollments in Coalfire. This may apply where scanning of completely different system structures are necessary. Consultation with OSC should be made to determine if multiple enrollments are appropriate.

Multiple Business Processes – Single Online SAQ

In some cases, a participant may have merchant card programs that function separately and have different business processes, to include different capture methods. As a result, when considered individually, each outlet may be eligible to complete a different Self-Assessment Questionnaire (SAQ), since there are four different SAQs to choose from (A, B, C, or D). The participant may elect to complete, <u>offline,</u> the appropriate SAQ that applies to an outlet's particular capture method. However, only one SAQ should be completed <u>online</u> through Coalfire, based on the consolidation of the individual SAQs completed offline. Whenever more than one SAQ is applicable to a participant, the questionnaire to complete on Coalfire should be the one that is most stringent.

Enrollment Process and Transition

It will be necessary for <u>all</u> participants (entities) to enroll in Coalfire at the chain level. Once the Pre-Enrollment Form is received, OSC will instruct Coalfire to pre-enroll the entity (at the chain level) in the Navis Portal. Upon being pre-enrolled in Coalfire, the entity's "Primary PCI Data Security Contact" identified on the Pre-Enrollment Form will receive a Welcome email from Coalfire Support with instructions to complete the enrollment via an online process. Upon receiving the Welcome email from Coalfire Support, the entity should complete the enrollment online. Some of the information needed to complete the online enrollment will include:

  - Capture method(s) being utilized
  - Annual card volumes of the chain
  - PCI Merchant Level that applies to the chain (Level 1, 2, 3, or 4)
  - Web facing IP addresses that require scanning (if applicable)

After enrollment is complete, the entity will be able to:

- Schedule its scans (if applicable)
- Complete the appropriate Self-Assessment Questionnaire (SAQ) online
- Add any additional users the entity desires to be able to view information on Navis Portal

Capture Methods Requiring Vulnerability Scanning

OSC has prepared a document entitled, “PCI Applicability to Card Capture Methods,” to assist entities in determining which card capture applications require vulnerability scans. The document can be viewed at:
http://www.osc.nc.gov/programs/pci/PCI_Applicability_to_Capture_Methods.pdf

Note that there are some IP addresses that no longer require scanning. The procedures required by Qualified Scanning Vendors to follow allow for certain "segmentation methods" to be used to "reduce the scope of the PCI Security Scan" (i.e., providing physical segmentation between the segment handling cardholder data and other segments; and employing appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments). A website that only has a link to a third-party service provider constitutes an appropriate separation from the cardholder environment referred to in the standard, as the two system components are not considered "connected." Therefore, from the perspective of the PCI DSS requirements, such website does not have to be scanned to obtain compliance.

Monitoring of Validation of Compliance

The merchant card processor / acquirer (i.e., SunTrust Merchant Services) is the party charged by the card associations with the responsibility to periodically obtain attestation of validation of compliance from the merchant (agency). The online process through Coalfire not only provides the ability for the entity to “attest” the validation of its scanning results on a quarterly basis, but it also allows the entity to “attest” the validation of its successful completion of the appropriate Self-Assessment Questionnaire (SAQ) on an annual basis. Such attestation responsibility is that of each entity.

The Office of the State Controller (OSC) has the capability to view the validation of compliance status of all chain numbers enrolled in Coalfire. Accordingly, OSC has the capability to generate management reports regarding the validation status of the various chain numbers: 1) Compliant; 2) Non-Compliant; or 3) Incomplete. The role of OSC will not be to ensure that validation of compliance has been performed, but to facilitate the reporting (attestation) of the validation of compliance status to STMS. Periodic reports will be provided to STMS. Such reports may be on a scheduled basis (likely monthly), or on an “as requested” basis as may be requested by one of the card associations.

SunTrust Merchant Services (STMS) will determine any rectifying action that may be needed by an entity whose chain indicates a non-compliant status. STMS may contact the entity directly regarding non-compliance issues. Should one of an entity’s multiple outlets result in the “chain” reflecting a non-compliant status, STMS may request information on the non-compliant outlet. Non-compliant outlets will be dealt with on an individual basis.

Since compliance with the PCI Data Security Standard is a policy of OSC for entities participating in the master services agreement with STMS, and considering the consequences of non-compliance, OSC deems it appropriate to advise appropriate central oversight agencies with management reports to assist them in their oversight responsibilities. Appropriate management reports may be submitted as follows:

- Universities – To UNC General Administration
- Community Colleges – To NC Community College System
- Local Units of Government and Local School Systems – To Local Government Commission

Questions

Questions regarding this process should be addressed to osc.pcicompliance@osc.nc.gov.