

Responding to a Notice of Non-Compliance with PCI Data Security Standard

Intent of Document

This document is intended to assist a participant in the State's Merchant Card Services Master Agreement who has received notification from either the State Controller, SunTrust Merchant Services, or a central oversight agency, indicating that the participant has not completed all necessary steps to be validated compliant with the PCI Data Security Standard (PCI DSS).

Reference Links to Requirements

State Controller's Memo - Dated June 19, 2008

http://www.osc.nc.gov/programs/pci/061908_PCI_Validation_Services_Memo.pdf

Validation of PCI Data Security Requirements – Dated June 19, 2008

http://www.osc.nc.gov/programs/pci/PCI_Validation_Requirements.pdf

State Controller's Memo – Dated October 1, 2008

http://www.osc.nc.gov/SECP/SECP_News.html

Compliance with PCI Data Security Standards Policy – Dated October 1, 2008

http://www.osc.nc.gov/SECP/SECP_Policies.html

Action Steps to Take

Step One – Determine the name of the individual who has been designated as the PCI Data Security contact for your entity. The name of the individual should be denoted on the "PCI Data Security Validation Services Pre-enrollment Form" filed with the Office of the State Controller (OSC) by your entity. If uncertain who has been designated, contact the State Controller's Office (OSC) to ascertain the name of the individual shown in OSC's Participant database.

Step Two – Determine if the PCI contact is aware of your entity's status as reflected on the TrustKeeper portal. The status could be one of the following four:

- Incomplete - Pending – Entity has been pre-enrolled, but the PCI contact has not yet logged in to the portal to complete the registration.
- Incomplete - Active – PCI contact has logged in to the portal and completed the registration, but has not completed one or both of the following: 1) Taken the online Self Assessment Questionnaire (applies to all entities); and/or 2) Scheduled vulnerability scans for public IP addresses (if applicable).
- Non-Compliant - Active – PCI contact has attempted to validate compliance but has failed, one or both of the following: 1) To complete the Self-Assessment Questionnaire (SAQ) successfully; and/or 2) To pass the vulnerability scan successfully.
- Compliant - Active – PCI contact has performed both tasks successfully: 1) Completed the Self-Assessment Questionnaire (applies to all); and 2) Passed the vulnerability scan (applies only to entities with card capture applications having public IP addresses).

Step Three – Determine which task (compliance program) your entity is required to complete (to be enrolled in), and then determine if your entity is registered accordingly in the TrustKeeper portal. You should be enrolled in one of the two compliance programs available:

- 1) Self-Assessment Questionnaire (SAQ) Only; or
- 2) SAQ and Vulnerability Scanning

Determination of which task/program applies to your entity's capture method(s) can be determined by referring to the chart viewed at the following link:

http://www.osc.nc.gov/programs/pci/PCI_Applicability_to_Capture_Methods.pdf

Determination of which program your entity has actually been enrolled in on the TrustKeeper portal can be viewed by logging into the portal. The portal will reflect enrollment as either:

- 1) PCI – Questionnaire Only; or 2) TrustKeeper PCI – Scanning and SAQ

Step Four – Determine which of the four Self-Assessment Questionnaires (SAQs) your entity is required to complete (for the chain) – A,B, C, or D. Refer to the chart at the following link to assist in making this determination: http://www.osc.nc.gov/programs/pci/PCI_Applicability_to_Capture_Methods.pdf

Step Five - Take action in accordance with the status that applies below.

Incomplete-Pending Status

- Ascertain if the entity's PCI contact has ever received the welcome email from TrustKeeper Support, as the welcome email has the login information. (Multiple emails have previously been sent to the PCI contact on file.)
 - It is possible that the emails have been going to your entity's spam folder.
 - It is possible that the emails have been going to the incorrect email address.
 - If another email is needed, contact OSC Support to obtain a copy of the welcome email.
 - Have the email address on file with OSC corrected if necessary.
 - Have the email domain "white listed" so future emails will not be filtered.
- If the welcome email has been received (or once it is received) by the entity's PCI contact, the PCI contact should log on to the TrustKeeper portal and complete the registration.
- Once the registration is completed, the online Self-Assessment Questionnaire (SAQ) should be taken. If unable to answer all questions satisfactorily, you can re-take the SAQ at a later time.
- If the entity is enrolled in the Scanning and SAQ program:
 - The IP address(es) to be scanned should be entered during the registration process
 - The vulnerability scan should be scheduled through the portal.
- Once the SAQ and any applicable scans are completed, you should re-ascertain your status, which will be one of those described below. Refer to the status below to determine what further steps need to be taken.

Incomplete – Active Status

- If your entity should be enrolled for the "Self-Assessment Questionnaire (SAQ) Only," and:
 - If enrolled correctly in TrustKeeper, complete the SAQ online; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning & SAQ), contact OSC Support and have the enrollment in TrustKeeper corrected.

- If your entity should be enrolled for the Scanning and SAQ, and:
 - If enrolled correctly in TrustKeeper, ensure the correct IP addresses to be scanned are registered, complete the SAQ; and schedule the scan; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning Only), contact OSC Support and have the enrollment in TrustKeeper corrected.
- If you have completed the SAQ, but have a “fail” status, take necessary remediation actions to be able to complete the SAQ successfully, as noted on the Compliance Questionnaire Report.
 - If modifications are made, you may attempt to complete the SAQ again to obtain a “pass” status. You are cautioned to answer the questions truthfully.
 - If modifications are not made, you will be subject to the consequences associated with not being compliant.
- If you have attempted the vulnerability scan, but have a “fail” status, take necessary remediation actions to be able to complete the scan successfully, as noted on the Full Scan Report.
 - If modifications are made, you may request TrustKeeper Support to perform a “directed scan” to attempt to obtain a “pass” status.
 - If modifications are not made, you will be subject to the consequences associated with not being compliant.

Non-Compliant – Active Status

- Determine if your non-compliant status is due to:
 - Failed the Self-Assessment Questionnaire (SAQ); or
 - Failed the vulnerability scan; or
 - Failed both.
- If your entity is enrolled for the “Self-Assessment Questionnaire (SAQ) Only,” determine if you incorrectly listed one or more domain names when you completed your registration.
 - Entering a domain name may cause TrustKeeper to expect that a scan should be performed and cause a non-compliant status to appear.
 - Contact TrustKeeper Support and have the domain name(s) removed from the registration setup.
- If your entity should be enrolled for the “Self-Assessment Questionnaire (SAQ) Only,” and
 - If enrolled correctly in TrustKeeper, complete the SAQ online; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning & SAQ), contact OSC Support and have the enrollment in TrustKeeper corrected.
- If your entity should be enrolled for the Scanning and SAQ, and:
 - If enrolled correctly in TrustKeeper, ensure the correct IP addresses to be scanned are registered, complete the SAQ; and schedule the scan; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning Only), contact OSC Support and have the enrollment in TrustKeeper corrected.
- If you have completed the SAQ, but have a “fail” status, take the necessary remediation actions to be able to complete the SAQ successfully, as noted on the Compliance Questionnaire Report.
 - If modifications are made, you may attempt to complete the SAQ again to obtain a “pass” status. You are cautioned to answer the questions truthfully.
 - If modifications are not made, you will be subject to the consequences associated with not being compliant.

- If you have attempted the vulnerability scan, but have a “fail” status, take the necessary remediation actions to be able to complete the scan successfully, as noted on the Full Scan Report.
 - If modifications are made, you may request TrustKeeper Support to perform a “directed scan” to attempt to obtain a “pass” status.
 - If modifications are not made, you will be subject to the consequences associated with not being compliant.

Compliant – Active Status

- Congratulations. You are compliant.
 - Retain copies of the Compliance Questionnaire Report for your files
 - Continue the steps below to see if you are enrolled correctly in TrustKeeper.
- If your entity should be enrolled for the “Self-Assessment Questionnaire (SAQ) Only,” and
 - If enrolled correctly in TrustKeeper, no further action is necessary; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning & SAQ), contact OSC Support and have the enrollment in TrustKeeper corrected.
- If your entity should be enrolled for the Scanning and SAQ, and:
 - If enrolled correctly in TrustKeeper (including having the proper IP addresses registered), no further action is necessary; or
 - If enrolled incorrectly in TrustKeeper (i.e., Scanning Only), contact OSC Support and have the enrollment in TrustKeeper corrected.

Notification from Merchant Card Processor

If you fail to obtain the “Compliant – Active” status, your entity’s name will be reflected on validation reports that are periodically provided to the merchant card processor (i.e., SunTrust Merchant Services), as well as to the applicable central oversight agency.

In accordance with the policy entitled, “Compliance with PCI Data Security Standards:”

Any participant receiving communications from the merchant card processor regarding a PCI Data Security non-compliance issue must respond to the processor within a reasonable time. Corrective actions must be taken that satisfies the processor’s concerns. Actions taken may include, but not be limited to:

- Correcting the non-compliance issue within the timeframe agreed to by the processor
- Implementing compensating measures agreed to by the processor
- Temporarily suspending the use of a merchant card capture application until the non-compliance issue is resolved
- Discontinuing the merchant card capture application altogether

Questions and Support

Office of State Controller’s Support Services Center

Telephone (919) 875-HELP (4357)

Email: OSC.secp.info@osc.nc.gov

TrustKeeper Support

<https://www.trustwave.com/support.php>