



State of North Carolina Office of the State Controller

Michael F. Easley, Governor

Robert L. Powell, State Controller

June 19, 2008

MEMORANDUM

TO: Agency Fiscal Officers
University Vice Chancellors
Community College Business Officers
Local Units of Government Finance Officers

FROM: Robert L. Powell, State Controller

A handwritten signature in black ink, appearing to read "Robert L. Powell".

SUBJECT: Validation Services - Compliance with the PCI Security Data Standard

I am writing to update you on some new processes regarding the State's security validation for merchant cards. As most of you are aware, the State of North Carolina has a Master Services Agreement (MSA) with SunTrust Merchant Services (STMS), dated August 1, 2006, allowing eligible entities (agencies, universities, community colleges, and local units of government) to subscribe to merchant card processing services. Under the MSA, the Office of the State Controller (OSC) functions as "facilitator" of the separate and individual arrangements made between participating entities and STMS. Accordingly, each participating entity is separately and individually responsible for adhering to the requirements of the MSA.

Upon enrolling in the MSA, each entity was advised that participation in the MSA would require the entity to become compliant and to remain compliant with the PCI Data Security Standard (PCI DSS), which is a requirement of the card associations. The primary focus of the PCI DSS is to help merchants improve the safekeeping of cardholder information by tightening their overall security standards, which in turn reduces their chances of experiencing security breaches, fraud, and potential catastrophic financial losses. Merchants found to be non-compliant with the PCI DSS are subject to substantial fines and penalties.

Under a statewide contract arrangement that OSC has with Trustwave Corporation, a qualified security assessor (QSA), participating entities are able to subscribe to a "Compliance Validation Service." The service provided has two components:

- 1) Vulnerability Scanning Service – For those entities requiring Web-facing IP addresses to be scanned; and
- 2) Remote Validation Service – For entities required to validate their compliance through the online "Self-Assessment Questionnaire" (SAQ) process

MAILING ADDRESS
1410 Mail Service Center
Raleigh, NC 27699-1410

Telephone: (919) 981-5454
Fax Number: (919) 981-5567
State Courier: 56-50-10
Website: www.ncosc.net

LOCATION
3512 Bush Street
Raleigh, NC

Since July 2005, entities that have needed the vulnerability scanning service (primarily for Web applications and POS software applications) have been enrolled in the portal provided by Trustwave, which is referred to as TrustKeeper. By virtue of subscribing to the scanning service, those entities have also had the added benefit of receiving the "remote validation service" as well. TrustKeeper has not been offered to entities that do not require scanning services. Consequently, those entities have not had the benefit of receiving the "remote validation service" [ability to complete the annual Self-Assessment Questionnaire (SAQ) online electronically.] If completed at all, those entities have had to complete the annual SAQ off-line in a paper format.

The Office of the State Controller now deems it appropriate to more fully utilize the services available from Trustwave. The enhancement will:

- 1) Allow all participants in the MSA with STMS to subscribe to Trustwave's Validation Service, not just those participants that require scanning services;
- 2) Provide a mechanism for all participants to be able to meet the PCI DSS requirement which specifies that the merchant is to "attest its validation of compliance" annually by completing a Self-Assessment Questionnaire (SAQ);
- 3) Provide a process that prompts the entity to complete the SAQ annually on the designated anniversary date;
- 4) Provide a mechanism for relaying the entity's attestation of validation of compliance to STMS as may be requested;
- 5) Provide for a monitoring process that allows applicable central oversight agencies to be aware of any non-compliance situations.

To transition to this new process, effective July 1, 2008, all participants in the Merchant Services Agreement with STMS are required to enroll in TrustKeeper, even if scanning services are not needed. To complete the process, the instructions provided on the following website link should be followed. http://www.ncosc.net/programs/pci/PCI_Validation_Requirements.pdf.

Please note that the instructions apply to those participants that are currently enrolled in TrustKeeper as well as to those that are not currently enrolled. For those that are currently enrolled, enrollment will be done at the "chain" level, not at the "outlet" level as is currently the case.

We are pleased that OSC can continue to offer this "Compliance Validation Service" on a statewide basis and that we can now more fully utilize the services available under the contract. In today's environment, it is ever more critical that we take the responsibility of securing cardholder data seriously. Addressing PCI compliance is not just a matter of avoiding noncompliance fines, it is about good business: reducing risk and preserving the trust of the citizens conducting business with the State.

More information can be found at: http://www.ncosc.net/programs/risk_mitigation_pci.html. Any questions may be addressed to OSC's Support Services Center, telephone (919) 875-HELP (4357).

cc: Agency's Primary PCI Data Security Contact