



State of North Carolina Office of the State Controller

Michael F. Easley, Governor

David McCoy, State Controller

November 13, 2008

MEMORANDUM

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

FROM: David McCoy *David McCoy*

SUBJECT: PCI Data Security Webinars and Compliance Requirements

I am writing to let you know about an upcoming webinar that contains important information for all governmental entities that accept credit cards, particularly those participants in the statewide enterprise solution offered by the Office of the State Controller (OSC).

While offering citizens the ability to make payments via credit and debit cards is considered a best business practice, there are high risks associated with the practice, primarily the risk that cardholder data could be stolen. Hardly a week goes by where there is not a news article regarding a security breach involving a major corporation or retailer. Not only could a security breach incurred by a government entity result in identify theft for citizens, but could also result in significant fines for the government entity.

Under a master services agreement with SunTrust Merchant Services (STMS), the OSC allows eligible entities to secure merchant card processing services from STMS. A prerequisite for participating in the MSA is compliance with the PCI Data Security Standard (PCI DSS). The PCI DSS is a comprehensive set of requirements established by the PCI Security Council, an organization founded by the major card brands. Compliance with the PCI DSS is critical in preventing potential security breaches, avoiding fines levied by card brands and avoiding termination of card processing services received from STMS.

To assist entities that are participants in the master services agreement with STMS, the OSC has acquired the services of Trustwave, a qualified security assessor to "validate" the participants' compliance with the PCI DSS. All participants have been pre-enrolled in the service provided by Trustwave. They have also been provided with instructions on how to complete the enrollment and to perform the necessary actions to be validated as "compliant" through the online portal provided by Trustwave. Information on the PCI DSS and the validation service can be viewed at the following hyperlink:
http://www.osc.nc.gov/programs/risk_mitigation_pci.html

The PCI Security Standards Council has announced the offering of a webinar entitled, "Understanding the PCI DSS Version 1.2." Version 1.2 of the standard was released October 1, 2008. Information on registering for the upcoming webinar (November 25 and December 17) can be viewed at the following

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.osc.nc.gov

LOCATION
3512 Bush Street
Raleigh, NC

hyperlink: <https://www.pcisecuritystandards.org/education/webinars.shtml>. Past webinars produced by the Council are also available at the website.

There is considerable information regarding the PCI Data Security Standard on the websites of both the Office of the State Controller and PCI Security Council. The policy issued by this Office on October 1, 2008 entitled, "Compliance with PCI Data Security Standards," provides further guidance on the process of governmental entities becoming compliant with the PCI DSS. The policy can be viewed at the following hyperlink: http://www.osc.nc.gov/SECP/Compliance_with_PCI_Data_Security_Standards.pdf

In addition, the appropriate central oversight agency having governance over your entity's Information Technology security should be consulted regarding any technical assistance that may be needed. This would include the NC Office of Information Technology Services, the NC Community College System, and UNC General Administration. The respective central oversight agency has more familiarity with the constituent entities' IT infrastructures and payment applications. In the case of local units of governments, guidance may be available from several sources, including the UNC School of Government.

All governmental entities' adherence to the PCI Data Security Standard is extremely important and I encourage the management of all government entities to take the necessary steps to ensure compliance. For those entities participating in the State's master services agreement with SunTrust Merchant Services, validation of your compliance through the service provided by Trustwave is critical in meeting your fiduciary responsibility of securing cardholder data. If your entity has not yet obtained the "compliant" status through the portal provided by Trustwave, I encourage you to place a priority on doing so.

For those entities not participating in the State's master services agreement with SunTrust Merchant Services, you should consult with your merchant card processor regarding the validation requirements that may apply to your entity, functioning as a merchant.

cc: Ann Garrett, State Chief Security Information Officer
NC Office of Information Technology

Jay Baucom, Associate VP for Information and Technology
NC Community College System

John Leydon, VP for Information Technology and CIO
UNC General Administration

Shannon Tufts, Director of Center for Public Technology
UNC School of Government

Ryan B. Draughn, Chief Information Officer
NC League of Municipalities

Rebecca Troutman, Intergovernmental Relations Director
NC Association of County Commissioners

Vance Holloman, Deputy State Treasurer
State and Local Government Finance Division
Department of State Treasurer

Agency Chief Information Officers

University Chief Information Officers