



# State of North Carolina Office of the State Controller

Michael F. Easley, Governor

Robert L. Powell, State Controller

July 14, 2005

To: Payment Card Merchants – Point of Contact  
SunTrust Merchant Services State Contract

From: Robert L. Powell  
State Controller

Subject: Payment Card Industry's Security Standards Program

As you may already know, the Office of the State Controller (OSC) is statutorily charged with implementing and managing the State's Electronic Commerce and Payments Program. As defined in North Carolina General Statute 147-86.20, electronic payments are payments by charge card, credit card, debit card, or by electronic funds transfer. To facilitate the State's Electronic Commerce and Payments Program, OSC entered into a contractual relationship with SunTrust Merchant Services, a partnership between SunTrust Bank and First Data Merchant Services to process credit and debit card payments. You are receiving this letter as a result of your entity's participation in the State's contract with SunTrust Merchant Services to process your electronic commerce transactions.

The growth of electronic commerce is bringing with it increasing occurrences of stolen cardholder information, which presents a significant concern to all constituencies using the electronic payment network. This rise in cardholder information compromises is driving increased focus and regulatory actions by the major card associations to ensure that cardholder data, as well as the payment network, is protected and kept secure. To counteract this problem, and to improve the integrity and security posture of the payment system, each of the leading card associations are requiring that merchants become compliant with the Payment Card Industry (PCI) Security Standards. The primary focus of the PCI Security Standards 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. Both Visa and MasterCard have mandated compliance of certain information security requirements for any merchant that "transmits, stores, accesses, or processes" cardholder information. Merchants found to be non-compliant with the respective security requirements may be subject to substantial fines and penalties. More information about the Visa and MasterCard Programs can be obtained by clicking on the following links: (VISA) [www.visa.com/cisp](http://www.visa.com/cisp) or (MasterCard) <http://sdp.mastercardintl.com>.

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](http://www.ncosc.net)

LOCATION  
3512 Bush Street  
Raleigh, NC

An Equal Opportunity/Affirmative Action/Americans With Disabilities Employer

Compliance requirements for merchants are determined by annual transaction volumes. The table below defines the four merchant levels.

Merchant Level	Description
1	<ul style="list-style-type: none"> <li>◆ Any merchant - regardless of acceptance channel-processing over 6,000,000 transactions per year.</li> <li>◆ Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</li> </ul>
2	<ul style="list-style-type: none"> <li>◆ Any merchant processing 150,000 to 6,000,000 e-commerce transactions per year.</li> </ul>
3	<ul style="list-style-type: none"> <li>◆ Any merchant processing 20,000 to 150,000 e-commerce transactions per year.</li> </ul>
4	<ul style="list-style-type: none"> <li>◆ Any merchant processing fewer than 20,000 e-commerce transactions per year.</li> </ul>

Based upon the merchant level determination, the PCI has also defined the compliance validation requirements. The following table details the validation requirements.

Level	Validation Action	Validated By	Due Date
1	<ul style="list-style-type: none"> <li>◆ Annual On-Site Security Audit</li> <li>◆ Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>◆ Independent Security Assessor or Internal Audit if signed by an officer of the entity</li> <li>◆ Qualified Independent Scan Vendor</li> </ul>	9/30/04
2 and 3	<ul style="list-style-type: none"> <li>◆ Annual Self-Assessment Questionnaire</li> <li>◆ Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>◆ Merchant</li> <li>◆ Qualified Independent Scan Vendor</li> </ul>	6/30/05
4	<ul style="list-style-type: none"> <li>◆ Annual Self-Assessment Questionnaire (Recommended)</li> <li>◆ Network Scan (Recommended)</li> </ul>	<ul style="list-style-type: none"> <li>◆ Merchant</li> <li>◆ Qualified Independent Scan Vendor</li> </ul>	TBD

***In order to ensure adequate personal identity and financial protection for the State's citizenry that elect to electronically transact their business with the State or a local government, to minimize the significant financial exposure resulting from fines and penalties imposed as a result of a security breach, and to ensure that all of the merchants falling under the purview of the State's master contract with SunTrust Merchant Services achieve compliance with the PCI***

**requirements, OSC has entered into a one-year contractual arrangement with AmbrionTrustWave (<http://www.atwcorp.com>) – a recognized industry leader in PCI compliance assessment solutions.** For the entities under the purview of the State Chief Information Officer, this compliance assessment complies with North Carolina General Statute (NCGS) §147-33.111 (c), which requires that the State Chief Information Officer and the State Auditor must authorize any contract involving a third-party vendor assessment of network vulnerability.

As noted in the above table, merchants were to be in compliance by June 30, 2005. OSC was not aware of the mandated deadlines until recently, therefore we were unable to meet the deadlines. We are, however, diligently working to ensure that **all** of the merchants falling under the State's master contract with SunTrust Merchant Services achieve compliance. Meeting the compliance standards of the various card associations can be a formidable challenge. OSC is requiring merchants **at all levels** (as defined in the table above) to complete the annual self-assessment questionnaire and to perform the required network scans for all externally-facing IP addresses. With regard to these network scans, even if an entity does not offer web-based transactions, there are other services that allow systems to be Internet accessible. Basic functions such as e-mail and employee Internet access will result in the Internet-accessibility of a company's network. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant systems if not properly controlled. If a merchant does not have any externally-facing IP addresses, then they will only be required to complete the annual self-assessment questionnaire.

OSC has arranged for AmbrionTrustWave to assist all merchants under the State's master contract with SunTrust Merchant Services with the completion of the annual self-assessment questionnaire and the performance of the required network scans. **These services will be performed at no additional cost to the merchants.** Through their TrustKeeper solution, AmbrionTrustWave will provide all merchants under the State's Master Contract with the ability to achieve a multi-card compliance program. TrustKeeper features a Policy Compliance tool and an Automated Vulnerability Scanning tool that brings together the critical components of Information Assurance (Standards, Policy, Compliance, and Audit) into a single, easy-to-use, web-based solution.

The TrustKeeper solution provides merchants with a web-based portal that:

- Allows easy enrollment into the Program.
- Collects security information about the merchant's systems and policies.
- Schedules and performs vulnerability scans.
- Provides easy-to-understand reports that track merchant compliance.
- Provides comprehensive customer support, access to remediation support, and online security resources.

In order to begin your compliance process, AmbrionTrustWave will be pre-registering your merchants into the TrustKeeper Portal. You will soon be receiving an email for each separate merchant under your purview from [support@trustkeeper.net](mailto:support@trustkeeper.net) with a link to register into the TrustKeeper Portal. This will be the first step in the merchant compliance process. You will need to distribute the pre-registration email to the appropriate merchant contact to complete the process. Each merchant will be responsible for completing the compliance validation process. Once the merchant receives the pre-registration email, they will need to:

1. Click on the registration link in the pre-registration email
2. Complete the registration questionnaire
3. Go to STEP 2
4. Complete the policy questionnaire – this includes 75 policy questions
5. Complete the network scan – you will need to include all externally-facing IP addresses

If you need assistance with the TrustKeeper Portal, please call 800-363-1621 (Customer Support) and they can assist you.

***IMPORTANT NOTE: You should consult your Chief Information Officer (CIO) or IT Director for assistance in the completion of the policy and network scan questionnaires. It is very important that you coordinate the dates and times of the network scans with your CIO or IT Director.***

Over the next several weeks, OSC will be scheduling weekly conference calls to assist you through your compliance process. ***The timeline for the initial completion and submission of both the policy and network questionnaire for your entity is July 28, 2005.*** The ***first conference call*** to address any issues encountered during the initial completion and submission of the questionnaires ***will be held on August 3, 2005 at 9:30 a.m.*** (additional details regarding this conference call will follow in a separate email). In order to facilitate this conference call, we ask that you ***submit your questions in advance via email to Ben McLawhorn***, OSC Risk Mitigation Services Manager, ***at [bmclawhorn@ncosc.net](mailto:bmclawhorn@ncosc.net) no later than the close of business on August 1, 2005.***

Thank you in advance for your efforts to ensure compliance with the PCI Cardholder Information Security Program requirements. If you require further assistance, or have any questions regarding the State's PCI Compliance Assessment initiative, please contact Ben McLawhorn, at (919) 981-5409 or via email at [bmclawhorn@ncosc.net](mailto:bmclawhorn@ncosc.net).

cc: The Honorable Leslie W. Merritt, Jr., State Auditor  
Mr. George Bakolia, State CIO