

Payment Card Industry Report on Compliance

Presented To:

North Carolina Office of the State Controller

August 12, 2011

Prepared By:

Christopher Lamm
(404) 932-5659
clamm@trustwave.com



Trustwave®
Information Security & Compliance

OSC Note:

This Report on Compliance (ROC) pertains to the State-operated Common Payment Service Gateway (CPS)

The Executive Overview below is published only, as detailed security information contained in the ROC is considered confidential pursuant to G.S. 132-6.1(c).

1. EXECUTIVE OVERVIEW

North Carolina Office of the State Controller has contracted with Trustwave to perform a Payment Card Industry (PCI) assessment to determine the compliance of their facilities with major Card Companies' published PCI security guidelines and requirements.

The PCI assessment process focuses solely on the security of cardholder data, whether North Carolina Office of the State Controller has effectively implemented information security policies and processes, and if there are adequate security measures to comply with the requirements to protect cardholder data. Additionally, the assessment reviews whether North Carolina Office of the State Controller is employing payment industry best-practices and provides recommendations for remediation of any non-compliant policies, processes, procedures, system configurations or vulnerabilities. This is ONLY an assessment and does NOT include professional services for remediation efforts.

As a result of this assessment, it was determined that North Carolina Office of the State Controller is COMPLIANT with PCI security requirements. A summary of North Carolina Office of the State Controller's "overall" compliance with card industry guidelines and requirements is provided in the following table

**Table 1-1. North Carolina Office of the State Controller
Overall PCI Compliance Summary**

PCI Section Title	Overall Compliance	Reference
Requirement 1: Install and Maintain a Firewall Configuration to Protect Data	YES	Section 7.1, Page: 16
Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters	YES	Section 7.2, Page: 37
Requirement 3: Protect Stored Data	YES	Section 7.3, Page: 49
Requirement 4: Encrypt Transmission of Cardholder and Sensitive Information Across Public Networks	YES	Section 7.4, Page: 71
Requirement 5: Use and Regularly Update Anti-Virus Software	YES	Section 7.5, Page: 75
Requirement 6: Develop and Maintain Secure Systems and Applications	YES	Section 7.6, Page: 81
Requirement 7: Restrict Access to Data by Business Need-to-Know	YES	Section 7.7, Page: 106
Requirement 8: Assign a Unique ID to Each Person with Computer Access	YES	Section 7.8, Page: 112
Requirement 9: Restrict Physical Access to Cardholder Data	YES	Section 7.9, Page: 136
Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data	YES	Section 7.10, Page: 146
Requirement 11: Regularly Test Security Systems and Processes	YES	Section 7.11, Page: 183
Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors	YES	Section 7.12, Page: 196