

Policy and Guidelines For Electronic Commerce

Office of the State Controller (OSC)		Effective Date: February 1, 2007
Policy Area: Electronic Commerce	Title: Merchant Cards Security Incident Plan	

Authority: Session Law 1999-434, Senate Bill 222, ratified in July 1999 amended various statutes, authorizing state government agencies to maximize the acceptance of electronic payments, a term which includes credit / debit cards (merchant cards) and electronic fund transfer (EFT). Electronic payments involve both inbound and outbound flows of funds. The primary statutes pertaining to the utilization of electronic payments for State agencies include: G.S. 147-86.10; G.S. 147-86.11(h); G.S. 147-86.20; G.S. 147-86.22; and G.S. 143B-426.40G(a).

Statutes authorizing the Office of the State Controller to issue policies regarding electronic payments include G.S. 143B-426.39(1) and (5); G.S. 147-86.11(a); and G.S. 147-86.22(b).

“Electronic Commerce in Government” is covered under Chapter 66, Article 11A (G.S. 66-58.1 through 66-58.19). G.S. 66-58.12 encourages the utilization of electronic transactions, including those initiated through the Internet, and requires consideration of security and privacy issues. Other applicable statutes include G.S. 132 (Public Records Law) and G.S. 14-113.24 pertaining to credit card numbers.

Program Administration: The State of North Carolina business environment includes all agencies, institutions, departments, bureaus, boards, commissions, and other entities subject to the Cash Management Law, as specified in G.S. 147-86.10. Although state agencies offer diverse services, North Carolina intends to use a statewide enterprise approach for the utilization of electronic payments.

Statutory Requirements:

G.S. 14-113.20 defines the “identifying information” that is subject to the Identity Theft Protection Act, which includes but is not limited to, “credit card numbers” and “debit card numbers.”

G.S. 75-61(14) defines a “security breach” as, “An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.”

G.S. 114-15.1 requires that the State Bureau of Investigation receive written notification of any information or evidence of "damage of, theft from, or theft of, or misuse of, any state-owned personal property." This reporting requirement includes reports of a security threat or breach of the state's information systems.

G.S. 147-33.113 requires the head of each State agency to cooperate with the State Chief Information Officer in the discharge of his or her duties by, “Providing the full details of the agency's information

technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation.”

G.S. 147-64.6(c)(18) requires the State Auditor, after consultation and in coordination with the State Chief Information Officer, to assess, confirm, and report on the security practices of information technology systems.

Reference:

IT Security Office - <http://www.iso.scio.nc.gov/InformationSecurityIncidentReporting.htm>

PCI Security Standards Council - <https://www.pcisecuritystandards.org/>

Policy: All participants in the State Controller’s Master Services Agreement for Merchant Card Services, as well as State agencies engaging in separate arrangements, are to devise a security incident response plan that incorporates the requirements of the Payment Card Industry Security Council. For those State agencies falling under the purview of The State Chief Information Officer, the incident response requirements defined by the Office of Information Technology Services (ITS) should also be incorporated.

- The agency’s incident response plan must include the requirements of the Payment Card Industry Data Security Standard (PCI DSS):
 - Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies.
 - Test the plan at least annually.
 - Designate specific personnel to be available on a 24/7 basis to respond to alerts.
 - Provide appropriate training to staff with security breach response responsibilities.
 - Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
 - Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
- The agency’s plan must include the notification requirements of the various State governing agencies as applicable.
 - In all cases, notify the Office of the State Controller within 24 hours of a known or suspected security breach.
 - If the agency falls under the purview of The State Chief Information Officer), and if the incident involves technology systems, notify the ITS Information Security Office, within 24 hours of a known or suspected security breach, and in accordance with the procedures specified by the Statewide Incident Management Plan.
- In accordance with the card associations rules, each card association and proprietary card company is to be notified whenever a security breach is known to have occurred or is suspected to have occurred. Notification is to be made through the merchant card processor. Requirements generally require a notification to be made within a specific timeframe, and an incident report to be submitted within a specific time frame.
 - If the agency is a participant in the State Controller’s Master Services Agreement for Merchant Card Services, the participant is to consult first with the Office of the State Controller (OSC), and the OSC shall make the appropriated notifications on the agency’s behalf, or advise otherwise.

- If the agency is not a participant in the State Controller's Master Services Agreement for Merchant Card Services, the agency shall consult with both the OSC and the merchant processor that it has contracted directly with regarding appropriate notifications.
- When reporting a security incident to the OSC, all pertinent details of the incident are to be provided to assist the OSC in making an assessment of the seriousness and extent of the incident. Any credit card data provided to the OSC as part of the assessment process shall be transmitted in a secure encrypted manner.
- Whenever a press release regarding the occurrence of a security breach is warranted, the OSC should be consulted first, in order to coordinate the timing of the release with any other notifications that may be required.
- In cases where a security incident is required to be reported to the card associations, the card associations may require a forensic investigation to be performed by a Qualified Security Assessor (QSA). For those agencies that are participants under the State Controller's Master Services Agreement, the participant may elect to use a QSA that the OSC may have a contract with to provide such services. Agencies are responsible for the costs of any forensic services provided.