

## ***Policy and Guidelines For Electronic Commerce***

<b>Office of the State Controller (OSC)</b>		Effective Date: August 16, 2000 Revision Date: November 1, 2007
<b>Policy Area:</b> Electronic Commerce	<b>Title:</b> Security and Privacy of Data	

**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. 66-58.12(a) states in part, “Public agencies...shall identify any inhibitors to electronic transactions between the agency and the public, including legal, policy, financial, or privacy concerns and specific inhibitors unique to the agency or type of transaction. An agency shall not provide a transaction through the Internet that is impractical, unreasonable, or not permitted by laws pertaining to privacy or security.”

G.S. 132-1.2(2), which pertaining to confidential information, states in part, “Nothing in this Chapter shall be construed to require or authorize a public agency or its subdivision to disclose any information that reveals an account number for electronic payment as defined in G.S. 147-86.20 and obtained pursuant to Articles 6A or 6B of Chapter 147 of the General Statutes or G.S. 159-32.1.”

G.S. 14-113.24 states in part, “Except as provided in this section, no person that accepts credit, charge, or debit cards for the transaction of business shall print more than five digits of the credit, charge, or debit card account number or the expiration date upon any receipt with the intent to provide the receipt to the cardholder at the point of sale...”

G.S. 132-1.8(a)(3) states, “When State and local governmental agencies possess social security numbers or other personal identifying information, the governments should minimize the instances this information is disseminated either internally within government or externally with the general public.”

**Policy:** All participants in any of the Master Services Agreements (i.e., Merchant Card Services and Electronic Funds Transfer Financial Services), as well as State agencies engaging in separate arrangements, are to adhere to the appropriate security and privacy requirements that may govern the entity. Notwithstanding any conflict with policies of The Office of Information Technology Services (ITS), the following requirements are to be adhered to:

- Each participant in a Master Services Agreement (MSA) must develop business and systems controls to ensure the confidentiality and integrity of financial transactions within their scope of electronic payment processing activities. Computer security measures, including physical security, logical application controls, transmission security, and firewall utilization where applicable, must be implemented to satisfy the integrity and confidentiality objectives as well as eliminating or reducing the general risks associated with computerized systems. All staff involved in the transaction of electronic business must be aware of the security requirements.
- In the case of state agencies, or non-state entities acquiring services through the Common Payment System (CPS), the requirements and policies of ITS that may be in effect at any time must be adhered to.
- Each participant requiring the services of the Common Payment System (whether for Merchant Card Services or EFT Processing Services) must, upon application, complete a security assessment survey, to assure compliance with ITS current requirements.
- Each participant utilizing a gateway service other than the Common Payment System (CPS), or performing direct transmissions or interfaces with a service provider (Merchant Card or EFT) must include any security requirements in its comprehensive IT security plan.
- In the case of Merchant Card services, each participant must:
  - Adhere to all applicable merchant card associations' operating rules (e.g., Visa, MasterCard).
  - Participate in any security assessments and security scans required by the associations and/or OSC, in order to be and to remain compliant with Payment Card Industry (PCI) Security Standards, and be responsible for any fines levied as the result of not being compliant.
  - If not utilizing the Common Payment Service, only utilize a third-party service provider that is compliant with Payment Card Industry Security Standards.
  - Store and protect cardholder data in accordance with industry standards, including not disclosing account information except on a "business need to know" basis or when compelled by law. Information that cannot be stored or retained includes: the 3-digit CVV 2/CVC 2 value located on the back of the card within the signature panel, and magnetic stripe data. In the case of Internet transactions, cardholder account numbers must not be transmitted to cardholders. All records containing account number information must be unreadable prior to discarding.
  - For point of sale transactions, adhere to the requirements of both applicable State law (G.S. 14-113.24) and the Payment Card Industry Security Standards pertaining to the printing of account numbers and expiration dates of cards on the cardholder's copy of the receipt. While the statutory requirements and the industry standards differ, the requirements of both can be met by only printing the last four digits. The merchant's copy of the receipt may or may not contain the full card number and expiration date, and should only contain the full number and expiration date if there is a business reason for doing so. The merchant copy of the receipts must be kept in a secure place (i.e. locked cabinet with minimal access) for eighteen months. At the end of the eighteen months, the receipts should be destroyed in a secure manner, preferably shredding.

- Maintain records of transactions in a manner that provides adequate security and audit trails, and in accordance with the agency’s official retention records, but at a minimum of at least eighteen months.
- In the case of Electronic Funds Transfer, each participant must:
  - Adhere to all security requirements of the ACH Originating Depository Financial Institution (ODFI), which generally include the requirement for the protection of passwords and access codes.
  - Adhere to all NACHA Operating Rules regarding the origination of ACH transactions.
  - Adhere to all NACHA Operating Guidelines relating to the origination of Internet-initiated entries (WEB entries). The Originator is required to establish procedures that provide for transactions to be handled in a “commercially reasonable manner.” Those aspects include commercially reasonable fraudulent transaction detection systems, security technology to establish a secure Internet session with at least 128 bit SSL encryption technology, and procedures to verify the validity of the RDFI’s routing number.
  - In the case of WEB entries initiated via the Internet, adhere to the NACHA Operating Rule requiring Originators to conduct an audit at least once per year to ensure that Receivers’ financial information is protected by security practices and that appropriate procedures are in place.
  - Adhere to all NACHA Operating Guidelines relating to the origination of Telephone-initiated (TEL entries). The Originator is required to utilize a commercially reasonable method (e.g., use of a directory, database, etc.) to verify the consumer’s name, address, and telephone number. The Originator is also advised to further verify the Receiver’s identity by verifying pertinent information with the Receiver (e.g., past buying history, mother’s maiden name, Caller ID information, etc.). Additionally, the Originator must establish commercially reasonable procedures to verify that routing numbers are valid.
- Each participant must comply with any specific confidentiality laws or regulations. Reference should be made to the requirements of the Department of Cultural Resources (DCR), identified as “Guidelines for Public Records,” found at <http://www.ah.dcr.state.nc.us/records/guidelines.htm> .
- Each participant must comply with any specific confidentiality laws as specified in the ITS publication, “Laws Relating to Confidential Records Held by North Carolina Government,” found at the DCR site referenced above.