



State of North Carolina Office of the State Controller

Michael F. Easley, Governor

Robert L. Powell, State Controller

November 27, 2007

MEMORANDUM

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

FROM: Robert L. Powell 
State Controller

SUBJECT: Policy Regarding Truncation of Merchant Cardholder Account Numbers

There are numerous requirements that governmental entities must adhere to as it relates to the securing of "identifying data" to prevent identity theft, which includes credit card and debit card account data (merchant cards). Some of the requirements are statutory, some are policy driven, and some are contractual. Entities that accept merchant cards are required by merchant agreements to adhere to the card association rules, as well as to any special requirements specified in the contracting vendor's "Operating Guide."

Regarding the printing of the cardholder's account number on sales slips, the requirement for the customer's copy is clear. As mandated by both Federal and State law, only the last four digits of the cardholder's account number can be printed on the sales slip, and the expiration date cannot be printed. However, regarding the printing of the merchant's copy of the sales slip, there are no statutory restrictions at this time, and the requirements may vary depending upon the vendor that the merchant uses to process the card transactions.

For those entities participating under the State's Master Services Agreement with SunTrust Merchant Services (STMS), Section 3.1 of the Operating Guide specifies that the complete cardholder's account number must be printed on the merchant's copy of the sales slip, while all except the last four digits of the account number are to be masked on the customer's copy. The Operating Guide further requires that the sales slips be retained for 18 months. This requirement is primarily to assist in resolving any disputed transactions at a later date.

Considering the risks associated with identify theft, the Office of the State Controller believes the STMS requirement-that the full cardholder's account number be printed on the merchant's copy of the sales slip-seems to go against the intent of the PCI Data Security Standard (PCI DSS), which encourages merchants to only store cardholder data if there is a business reason to do so. While it may be argued that there is a business case for retaining the complete account number, to assist in resolving disputed transactions, there are alternate means of identifying the account number if necessary.

The OSC has therefore successfully negotiated Amendment Number 1 to the Master Services Agreement, relieving a participating entity, at its option, from being required to print the entire cardholder account number

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

LOCATION
3512 Bush Street
Raleigh, NC

on the merchant's copy of the sales draft or credit voucher. The amendment can be viewed at the following link: http://www.ncosc.net/SECP/Amendment_No_1_NC_SunTrust_for_Truncation_09.01.07.pdf

As a result of the amendment, the E-Commerce policy entitled, "Security and Privacy of Data" has also been revised, to recognize the option now available to participants. The revised policy can be viewed at the following link: http://www.ncosc.net/Credit_Card/SecurityandPrivacyofData.pdf

Each participant in the MSA with STMS that utilizes POS terminals for face-to-face transactions should determine if there is truly a business need for printing the complete account number on the merchant's copy of sales slips and credit vouchers. If the business need does not outweigh the risks associated with storing the cardholders' account numbers, the participant should consider taking the appropriate steps to alter its procedures. The steps involve either: 1) acquiring new POS terminals having the capability to truncate the cardholder account number; or 2) reprogramming existing POS terminals to allow for the truncation.

Entities should be aware that not all POS terminals are capable of the "merchant copy truncation." The capability depends upon the make and model of the terminal. The manner in which the switch can be performed depends upon the connection platform at STMS. If the terminal is connected to the Nashville Platform, the switch can be performed centrally by STMS.

The following POS terminals are known to be terminals that are merchant copy truncation capable: VeriFone Omni 3750, Hypercom T-4100, First Data FD-100, and IC Verify Software. Should you have one of these terminals, and desire for them to be switched to the "merchant copy truncation" mode, contact STMS Technical Support Services, Tel: (800) 654-8819. Information to be supplied include: 1) outlet's merchant number; 2) terminal ID number; 3) make and model of POS terminal; and 4) terminal serial number.

Some commonly used older terminals that are not merchant copy truncation capable include: VeriFone Omni 3200, LinkPoint AIO, all VeriFone Tranz terminals, and all Eclipse terminals. Additionally, the Nurit 8000 wireless terminal is not merchant copy capable. Each entity utilizing any terminal that is not merchant copy capable should evaluate the factors associated with replacing the terminals, now or at some point in the future. It is highly suggested that any new terminals purchased be merchant copy truncation capable. Another term used to describe the capability is "double truncation." Terminals currently offered by STMS and the associated pricing can be found on Schedule B, at the following link: <http://www.ncosc.net/SECP/ScheduleB-ScheduleofFees.pdf>

Participants that utilize POS Software applications should contact the vendor that supplied the software to ascertain the steps required to modify the configuration to enable the merchant copy truncation feature (aka duplicate truncation).

Questions regarding the truncation policy may be addressed to the OSC Support Services Center at (919) 875-4357, or to Amber Young, Central Compliance Manager, at (919) 981-5481.

CAUTION: Several incidents of an apparent scam have been reported regarding individuals calling or faxing merchants advising that they should replace their POS terminals. The caller requests the merchant to provide a copy of their bank check in order to obtain their bank account number. Agencies should be cautious of any such unsolicited phone calls. It is not the practice of SunTrust Merchant Services to make such unsolicited phone calls.