

## Capture Solutions – Merchant Cards

Participants in the Merchant Card Program MSA have several methods that can be used to capture and transmit merchant card activity to SunTrust Merchant Services (STMS). The option(s) selected depends upon the type of transaction, and upon whether the transaction is for a “card-present” or a “card not-present” transaction. A participant may utilize more than one capture solution. Generally, each capture solution is assigned a different merchant number. A description of the various capture solutions follows.

### Point of Sale (POS) Terminal

- Used primarily for card-present transactions (card swiped). Can also be used for “card not-present” transactions if keyed.
- POS terminals can be purchased, rented, or leased (from STMS or vendor of choice).
- Requires dedicated analog telephone line to STMS.
- Business environment must comply with PCI Data Security Standard (SAQ B applies).
- PCI vulnerability scanning is not required for stand-alone POS terminal
- POS terminals available from STMS can be viewed at:  
[http://www.osc.nc.gov/EPP/Equipment\\_Fees.pdf](http://www.osc.nc.gov/EPP/Equipment_Fees.pdf)

### Point of Sale Software

- Used primarily for “card-present” transactions (card swiped). Can also be used for “card not-present” transactions if keyed.
- Requires utilization of PC and servers to capture and transmit transaction data in a batch mode, and involves external-facing IP addresses.
- POS software can be obtained from various vendors, but the application must be compliant with the “Payment Application Data Security Standard” (PA-DSS).
- Electronic cash register is the most common form of POS software.
- Interactive Voice Response (IVR) is a form of POS software.
- Associated external-facing IP addresses must be enrolled with the State’s Qualified Security Assessor (Trustwave) for vulnerability scanning purposes.
- Application must stay updated with the most current version of the software, and appropriate security patches, and remain PA-DSS compliant.
- If an off-the-shelf application is utilized, it must be listed on the PCI Security Council’s [List of Validated Payment Applications](#).

### Common Payment Service – Internet Capture

- Gateway solution provided to participants that has its own in-house website capture application.
- Used for “card not-present” transactions captured through the participant’s website.
- Agency is responsible for developing its own Web capture system.
- Utilizes Cybersource API to receive transaction data from participant and to transmit to STMS.
- CPS is a certified service provider, being compliant with the PCI Data Security Standard.
- Associated external-facing IP addresses must be enrolled with the State’s Qualified Security Assessor (Trustwave) for vulnerability scanning purposes.
- Business environment must also comply with PCI Data Security Standard (PCI DSS).
- CPS fee is \$.35 per transaction, invoiced by ITS.
- CPS information can be viewed at: [http://www.osc.nc.gov/SECP/SECP\\_CPS.html](http://www.osc.nc.gov/SECP/SECP_CPS.html)

### Common Payment Service – Virtual Credit Card Terminal

- Web based solution that allows for card transactions to be keyed online by the participant.
- Used for “card not-present” transactions, primarily mail order and telephone orders (MOTO).
- CPS VCCT is certified as being compliant with the PCI Data Security Standard.
- Business environment must comply with PCI Data Security Standard (SAQ A or B applies).
- CPS VCCT fee is \$.35 per transaction, invoiced by ITS.
- CPS VCCT information can be viewed at: [http://www.osc.nc.gov/SECP/SECP\\_CPS.html](http://www.osc.nc.gov/SECP/SECP_CPS.html)

### PayPoint Gateway Service

- Some participants desire a gateway service that also offers a Web capture component.
- PayPoint became available to participants from STMS in April 2009, pursuant to Amendment Number 2.
- PayPoint offers a web component also referred to as a “presentment engine.”
- Three major features include: 1) Portal Builder; 2) Electronic Biller Presentment; and 3) Multiple payment options (cards or ACH drafts)
- PayPoint is considered a service provider and is subject to [PCI Validation of Service Providers](#).
- Agency’s business environment must also comply with PCI Data Security Standard, but the associated PayPoint IP address is not subject to vulnerability scanning by Trustwave.
- Information on PayPoint may be viewed at: [http://www.osc.nc.gov/SECP/SECP\\_PayPoint.html](http://www.osc.nc.gov/SECP/SECP_PayPoint.html)

### Yahoo Store

- Web based solution that allows for Website to be listed as an NC@YourService Store on NCgov.com - <http://www.nc.gov/NCStore.aspx>
- Used for Internet captured transactions, where a shopping cart is needed.
- Yahoo is considered a service provider and is subject to [PCI Validation of Service Providers](#).
- Agency’s business environment must also comply with PCI Data Security Standard, but the associated Yahoo IP address is not subject to vulnerability scanning by Trustwave.
- Most agencies select the Starter Plan, hosted by Yahoo, suitable for transaction volume of less than \$12,000 per month.
- Starter Plan rates: Setup fee is \$50; monthly maintenance fee is \$39.95; transaction fee is 1.5%.
- Transactions settle through STMS, with all associated fees applying, in addition to Yahoo fees.
- Yahoo Store Solution information can be viewed at: <http://smallbusiness.yahoo.com/ecommerce/>

### Third-Party Gateway Service

- Some participants desire to utilize capture solutions (software or Internet) provided by third parties that require the utilization of a specific gateway service provider, instead of the Common Payment Service (CPS) gateway, the PayPoint gateway, or the Yahoo Store solution.
- If the OSC’s MSA is to be utilized, the selected gateway must be one supported by STMS.
- Some gateway vendors use their own merchant card processor, not STMS.
- The selected gateway must be one that has been pre-approved by OSC.
- Used for both “card-present” and “card not-present” transactions, but primarily Internet captured transactions.
- The third-party gateway, functioning as a service provider, must provide evidence that it is compliant with the PCI Data Security Standard.
- The associated web address may or may not have to undergo vulnerability scanning by Trustwave, depending upon where the servers are hosted, and whether the agency “stores” any cardholder data.
- Any convenience fees that may be charged must be approved by OSBM per G.S. 66-58.12.
- Refer to the OSC document pertaining to [PCI Validation of Service Providers](#).

**PCI Standard Applicability for each solution above:** Refer to: [PCI Applicability Chart](#)

### Implementation Plans

For each of the above capture solutions, a Project Implementation Plan is provided.

Common Payment Service	<a href="http://www.osc.nc.gov/SECP/CPSImplementationProjectPlan.xls">http://www.osc.nc.gov/SECP/CPSImplementationProjectPlan.xls</a>
All Other Solutions	<a href="http://www.osc.nc.gov/SECP/SECP_MerchantCard_Enrollment.html">http://www.osc.nc.gov/SECP/SECP_MerchantCard_Enrollment.html</a>

### Internal Policies and Procedures Template

Merchant Card Processing	<a href="http://www.osc.nc.gov/SECP/InternalPoliciesProcedures-Cards.doc">http://www.osc.nc.gov/SECP/InternalPoliciesProcedures-Cards.doc</a>
--------------------------	---