

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) Terminals

- 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).
- 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/SECP/POS Equipment Prices 6-1-15.pdf](http://www.osc.nc.gov/SECP/POS_Equipment_Prices_6-1-15.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 (Coalfire) 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.

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 Coalfire.
- Information on PayPoint may be viewed at: http://www.osc.nc.gov/SECP/SECP_PayPoint.html

Global Gateway e4 Solution

- Seamlessly integrate payment processing to your website
- Offers advanced payment functionality built for any size merchant
- Flexible and simple integration and setup options
- Available Interface Options:
 - Real-time Payment Manager (RPM) – secure, web-based system enables your internet connected computer to process individual or batch transactions, pull reports and administer options that fit your business needs
 - Hosted Checkout – quickly and easily add payment processing to your website with hosted customizable and secure checkout pages to collect sensitive billing information
 - Web Service API – allows merchant and/or third-party applications to process transactions through the gateway via a secure SSL encrypted session

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 PayPoint gateway or Global Gateway e4 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 Coalfire, 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](#)

For each of the above capture solutions, a [Project Implementation Plan](#) is provided.

Internal Policies and Procedures Templates: <http://www.osc.nc.gov/policy/EC/index.html>