Overview
This document is intended to provide guidance to a State entity desiring to accept credit and/or debit cards as a method of payment. The generic term for both types of cards is “merchant cards.”

The banking industry considers any entity accepting merchant cards to be a “merchant.” Accordingly, all merchants are required to:

- Utilize a merchant card provider to process the cards (for authorization and settlement)
- Adhere to all card brands’ rules (i.e., Visa, Mastercard, Amex, Discover)
- Be compliant with the Payment Card Industry (PCI) Data Security Standard (PCI-DSS)

The State has a statewide term contract with a single merchant card provider to service all State entities. The contract is with Fiserv’s “SunTrust Merchant Services, LLC” (STMS). Information regarding the contract is found below.

There are two categories of payment transactions that could apply:

- Card-present transactions (i.e., face-to-face, point-of-sale)
- Card-absent transactions (i.e., e-commerce, web payments)

Should card-absent transactions be utilized, it will be necessary for the entity to obtain a payment gateway service. Options for obtaining a payment gateway service can be through STMS or through SC.Gov, a web portal service provided by SC Interactive, LLC (SCI). Information regarding SC.Gov and other payment gateways is found below. Other payment gateway vendors may be considered only in accordance with applicable procurement rules.

Statewide Merchant Card Contract
Information about the statewide contract with STMS (contract number 4400011556) can be found at the following link:


To participate in the contract, an entity is required to execute the appropriate “Participation Agreement” (Exhibit G for State entities and Exhibit G-1 & G-1A for local units of governments). It is critical that the entity read all components of the statewide contract, as execution of the Participation Agreement bounds the entity to all terms.

Not all exhibits and schedules in the contract may apply, depending upon the features being subscribed to. The ones that apply to all participants are:

- Master Services Agreement
- Bankcard Addendum
- Schedule of Fees
- Menu of Services Available
- Point of Sale Terminals Available
- PCI Rapid Comply Service
Payment Gateways
Entities desiring to accept online payments will also need to acquire the services of a payment gateway vendor. A payment gateway supports an e-commerce application that allows an entity’s clients to initiate payments online via the web.

There is no single statewide contract for payment gateway services that entities are required to utilize. However, there are two statewide contracts that offer ancillary payment gateway services, under which gateway services could be subscribed to on an optional basis and without an additional procurement process:

- SunTrust Merchant Services (STMS) for merchant card processing
  - PayPoint
  - Payeezy
  - CardConnect
- SC Interactive (SCI) for Web portal services (SC.Gov)

A document entitled, “Payment Gateway Solutions Assessment” is found at the following link: https://treasurer.sc.gov/media/80639/Payment-Gateway-Solutions-Assessment.pdf

The document will assist in determining which payment gateway option is best for the entity. One of the decision points discussed in the document is whether a “service fee” (sometimes referred to as a convenience fee) will be levied against the cardholder. The options are:

- No service fee is levied against the cardholder. Entity is invoiced for the merchant card fees
- A service fee is levied and paid to the entity, used to offset the merchant card fees
- A service fee is levied, collected and retained by the vendor, who pays all card fees

If a service fee will be levied against the cardholder, there are several vendor options:

- SCI’s SC.Gov – For both ecommerce and POS transactions
- Touchnet PayPath - For universities
- STMS’s Service Fee Service – For use with PayPoint, CardConnect, or Payeezy payment gateways

In the case of ecommerce transactions, the vendor collects the service fee. The service fee is processed as a separate transaction under a MID belonging to the vendor. In the case of POS transactions, the service fee is normally collected by the participant under the participant’s MID and then subsequently remitted to the vendor.

SC Gov Web Portal
The statewide contract (number 5400007500) with SC Interactive (SCI) for the web portal SC.Gov is administered by the Department of Administration’s Division of Technology. Information regarding the contract can be found at the following links:
https://www.admin.sc.gov/technology/technology-operations/it-forums/e-gov-oversight-committee
http://webprod.cio.sc.gov/SCSolicitationWeb/solicitationAttachment.do?solicitnumber=5400007500
https://sc.gov/Pages/default.aspx

PCI Data Security Standard Compliance
Each entity functioning as a merchant is required by the card brands to be compliant with the Payment Card Industry Data Security Standard (PCI-DSS). Each entity should be aware of the following points:

- Compliance is a contractual obligation to STMS
- Failure to comply with the standard may result in substantial fines levied by the card brands
- Attestation of compliance through STMS’s PCI Rapid Comply tool is required
• STMS and STO monitors PCI compliance on an ongoing basis, with any extended non-compliance status requiring a written remediation plan
• Utilizing SC.Gov, or any other payment gateway, generally reduces the entity’s scope of compliance but does not eliminate it
• Three fundamental PCI compliance action items are required prior to STO allowing an entity to enroll: PCI policy; Security Incident Plan; and Employee Awareness Training.

The following links should be referred, to obtain a better understanding of the PCI-DSS:
https://treasurer.sc.gov/media/60083/PCI-Compliance-Roadmap-SC-July2016-002-.pdf
https://www.pcirapidcomply.com/faq.html

PCI Rapid Comply is a tool provided by STMS allowing the entity to attest its compliance:
https://www.pcirapidcomply.com/faq.html

**Merchant IDs (MIDS)**
Once enrolled, a participant (considered a legal entity) will be assigned a “primary” merchant ID (MID), sometimes referred to as a “head chain MID” or a “chain-chain number.” Under the primary MID, there will be at least one “outlet MID.” There could be multiple outlet MIDs, one assigned to each business unit, location, or payment channel. The participant’s primary MID and associated outlet MIDs can be viewed through STMS’s reporting tool (ClientLine). A participant’s PCI compliance attestation is done at the primary MID level.

<table>
<thead>
<tr>
<th>Enrollment Process - Merchant Card Bank Services Contract</th>
<th>Task</th>
<th>Reference / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Review the master statewide contract, including terms, optional services offered, and fee schedules</td>
<td>Available at SFAA Procurement Website. Schedule A lists all services. Schedules B and B1 list the service fees. Schedules C and D list the equipment fees. Schedule F is STMS’s Acceptance Guide. Other schedules pertain to optional services.</td>
</tr>
<tr>
<td>2</td>
<td>Review STO’s policies and documents pertaining to PCI</td>
<td>Available at the links above. PCI compliance is a prerequisite for participation in STMS’s contract.</td>
</tr>
<tr>
<td>3</td>
<td>Consult with STMS regarding card capture options</td>
<td>Obtain from STMS recommendations for equipment and capture devices suitable for procurement. Engage SCI in the discussions if SC.Gov will be utilized.</td>
</tr>
<tr>
<td>4</td>
<td>a Take three initial steps for PCI compliance</td>
<td>Three action items are required prior to STO executing the PA submitted. Develop a: PCI policy; Security Incident Plan; and Employee Awareness Training.</td>
</tr>
<tr>
<td></td>
<td>b Advise STO of 3 actions taken</td>
<td>Submit evidence to STO prior to or along with PA below.</td>
</tr>
<tr>
<td>5</td>
<td>a Execute and submit the appropriate Participation Agreement (PA)</td>
<td>Agreement to submit depends upon type of participant: Exhibit G – “Agency Participation Agreement” for State agency, university / college; Exhibit G-1 – “Political Subdivision Participation Agreement” for local unit of government.</td>
</tr>
<tr>
<td></td>
<td>b Execute “Additional Terms for Political Subdivision Participation Agreement”</td>
<td>Exhibit G-1A. Only applies to local units of government and not to State entities. Pertains to potential bankruptcy and potential requirement for establishment of a reserve account. Attach to Exhibit G-1. (STO is not a party to Exhibit G-1A)</td>
</tr>
<tr>
<td>c</td>
<td>Complete Schedule A – Menu of Services Available</td>
<td>Some menu items are provided to everyone and some are optional. Denote on the schedule all services desiring to subscribe to and attach to the Participation Agreement that is to be submitted.</td>
</tr>
<tr>
<td>d</td>
<td>Submit PA to STO</td>
<td>PA can be submitted via email to STO.</td>
</tr>
<tr>
<td>6</td>
<td>STO and STMS executes PA</td>
<td>After verification of the three initial PCI action items, STO will coordinate with STMS execution of PA.</td>
</tr>
<tr>
<td>7</td>
<td>a Complete Merchant Outlet Setup Form(s) provided by STMS. (Provided by SCI if SC.Gov is involved)</td>
<td>Complete a separate form for each outlet (line of business or location) to be established. Information is necessary for STMS staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine, Capture Method, Settlement bank account, billing information, statement rendering, etc.).</td>
</tr>
<tr>
<td>b</td>
<td>Select invoicing option</td>
<td>Invoicing can be at primary MID level (central billing) or at each outlet level. If SCI is utilized, SCI is invoiced.</td>
</tr>
<tr>
<td>c</td>
<td>Determine if Discover and/or Amex will be accepted</td>
<td>Visa and MasterCard are included in basic service. Discover and Amex each requires separate registration.</td>
</tr>
<tr>
<td>8</td>
<td>a Determine capture devices for card-present transactions</td>
<td>POS terminals or software. POS terminals are available from STMS. POS software may be obtained elsewhere.</td>
</tr>
<tr>
<td>b</td>
<td>Chip-enabled POS Terminals</td>
<td>Recommended</td>
</tr>
<tr>
<td>c</td>
<td>Encryption (E2E or P2PE) ?</td>
<td>Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional $.01 per transaction (See Schedule J of contract).</td>
</tr>
<tr>
<td>9</td>
<td>Determine gateway needed for card-absent transactions</td>
<td>If SC.Gov is utilized, obtain and execute appropriate SOW directly with SCI.</td>
</tr>
<tr>
<td>10</td>
<td>a Procure devices/software</td>
<td>From STMS or software vendor, and in some cases from SCI</td>
</tr>
<tr>
<td>b</td>
<td>Install &amp; test devices/software</td>
<td>Assisted by STMS or by software vendor</td>
</tr>
<tr>
<td>11</td>
<td>Designate PCI Point of Contact</td>
<td>Designation of PCI POC is required by supplemental policy. Advise and keep STO updated of POC.</td>
</tr>
<tr>
<td>12</td>
<td>Create a PCI Oversight Committee (Best Practice)</td>
<td>Such committee has the responsibility for identifying necessary actions to comply with the PCI Data Security Standard, using STO’s “PCI Compliance Roadmap” document for guidance. Sample charter is available from STO.</td>
</tr>
<tr>
<td>13</td>
<td>a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level)</td>
<td>Validation of compliance is reported and tracked via the portal. Enrollment is normally done by the PCI POC. If a QSA is involved, the participant could request STMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation.</td>
</tr>
<tr>
<td>b</td>
<td>Enroll IP addresses to be scanned</td>
<td>Applies if external-facing IP address are involved.</td>
</tr>
<tr>
<td>c</td>
<td>Validate compliance</td>
<td>Enrollment in PCI Comply should be prior to any card transactions. Validation of compliance (SAQ completion) is required within 90 days of implementation.</td>
</tr>
</tbody>
</table>

**Email Addresses:**
- STMS: [SC.Gov@FirstData.com](mailto:SC.Gov@FirstData.com)
- STO: [STOBankingDivision@sto.sc.gov](mailto:STOBankingDivision@sto.sc.gov)