SC State Treasurer's Office
PCI Data Security Compliance Roadmap
Revised October 2020

Objective and Overview

The objective of this document is to provide suggested procedural guidance (roadmap) for participants in the State Treasurer's Office (STO) statewide Merchant Bank Card Services contract to assist in complying with version 3.2 of the Payment Card Industry Data Security Standard (PCI DSS). The STO contract with SunTrust Merchant Card Services (STMS) is dated October 2015.

Guidance is appropriate considering the contract requires each participant to adhere to all card brand associations' rules, including the requirement to comply with the PCI Data Security Standard (PCI DSS), and of the possibility of fines for non-compliance. Additionally, the contract with STMS provides for a service known as "Clover Security," previously known as PCI Rapid Comply that allows a participant to validate its compliance with PCI DSS.

This document provides suggested guidance that is geared more towards the business user than the IT user. Accordingly, it is **not intended to be all inclusive, but to be a supplement to documents available from the PCI Security Council and to guidance that may be obtained from a Qualified Security Assessor (QSA).**

Guidance herein is based partially upon information available from the card brands' websites, and from the PCI Security Council's website which may be viewed at:
https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
https://www.pcisecuritystandards.org/pci_security/small_merchant

This document provides a discussion on:

- Source of compliance requirements
- The three components of PCI DSS compliance process
- PCI compliance process responsibilities
- Determining merchant card transaction volumes
- Identifying cardholder data environment
- Identifying third-party service providers
- Identifying card capture devices
- Identifying POS software applications
- Developing a security policy for dissemination
- Developing an employee awareness training program
- Developing a security incident plan
- Assessing the twelve areas of PCI DSS
- Determining penetration testing and internal vulnerability scanning requirements
- Validating compliance via Clover Security
- Extensive PCI related services
- Explanation of the eight SAQs
- Encryption Considerations

Completion of many of the tasks listed above may be necessary in order to successfully answer the Self-Assessment Questionnaire (SAQ) that the participant is required to prepare, either through Clover Security or otherwise.

1. Source of Compliance Requirements

Compliance with the PCI DSS is a contractual requirement of the merchant card services provider (SunTrust Merchant Services, LLC) and the acquirer bank (SunTrust Bank, N.A.), which jointly utilizes Fiserv as the processor. The standard, which is subject to revisions, is promulgated by the PCI Data Security Council.

2. The Three Components of PCI DSS Compliance Process

The PCI compliance process involves three components:

- Compliance – Performing required tasks and maintaining systems appropriately, which must be done throughout the year (not just an annual event).
- Validation – Preparing an annual Self-Assessment Questionnaire (SAQ) and performing any required external vulnerability scanning on a quarterly basis, if applicable.
- Attestation – Certifying compliance with the standard. Attestation can be through an online reporting tool or by completing and submitting an "Attestation of Compliance" (AOC).

3. PCI Compliance Process Responsibilities

Since merchant cards processing is associated with IT systems, financial systems, and business users, it is imperative that there be a coordination of all parties and activities involved in the validation process. PCI DSS compliance is a result of management's decision to accept merchant cards, and as such, this decision may require extensive support from IT. Thus, PCI DSS compliance is primarily deemed to be a business problem with an IT solution.

One of the best practices for ensuring a coordination of the interests and responsibilities of both sectors is to establish a PCI Oversight Committee. The creation of a committee charter is recommended. A sample charter is available from STO.

The other two components of the process (validation and attestation) are normally the responsibility of someone in the business sector. It is the business sector that is responsible for adhering to accounting, administrative, and procurement policies. Additionally, it is someone in the business sector that is involved in the execution of the contractual arrangement with the merchant card provider and will be addressing any issues that may result from non-compliance or breaches (e.g., inquiries from the card brands or law enforcement agencies).

4. Determining Merchant Card Transaction Volumes

The card brands, not the PCI Security Council, determine what merchants must do in order to validate their PCI compliance. The determination is based upon annual transaction volumes. There are four established levels under which a merchant will fall: 1, 2, 3, or 4. All participants in the State's contract are currently either a Level 3 or 4 merchant.

A) Level 1 and 2 merchants

Level 1 merchants are required to have an annual onsite security audit performed by a qualified security assessor (QSA). Level 2 merchants are required to have either an annual onsite security audit performed by a qualified security assessor (QSA) or a passing Self-Assessment Questionnaire (SAQ) along with a corresponding Attestation of Compliance (AOC). If a PCI Approved Qualified Security Assessor (QSA) is engaged to assist with the preparation of the merchant's SAQ, the QSA must come on-site.

As an alternative, Level 2 merchants may choose to complete a Self-Assessment Questionnaire using an internal security auditor (ISA). In order to use an internal auditor, the merchant must ensure that the primary internal auditor staff person engaged in validating PCI DSS compliance attends PCI SSC ISA training and passes the associated accreditation program annually.

In addition, level 1 and 2 merchants must undergo external vulnerability scanning, if applicable (utilize capture systems involving external/public facing IP addresses).

B) Level 3 and 4 merchants

Level 3 and 4 merchants must complete an annual self-assessment questionnaire (SAQ) and undergo external vulnerability scanning, if applicable. On-site security audits are not necessarily required of level 3 and 4 merchants.

C) Transaction volumes

The transaction volume used in determining the appropriate merchant level is that of the "doing business as" (DBA) entity, which in most cases is associated with the participant's primary merchant ID (MID) level, not individual outlet MID levels, departments, or payment channels. Under the State's master contract, STMS/Fiserv monitors each participant's transaction total volume and e-commerce volume and makes the official determination of the participant's PCI level.

A participant can ascertain its annual transaction volume, for each card brand, through all payment channels, to determine its assigned merchant level. Each brand specifies calculating its own card transaction volume only to determine the assigned level. However, the brand with the lower volume defers to the brand with the higher volume as the level that is to be assigned. For example, most participants will have more Visa transactions than MasterCard

transactions. Those participants will therefore use the Visa transaction volume to determine its assigned level. Total transaction volumes across all brands are not to be considered.

The following exercise will assist in determining which level you are likely considered. Transaction volumes can be determined through the merchant card processor's online reporting tool (e.g., ClientLine) and from reports provided by any gateway services utilized.

Annual Merchant Card Transactions Volume					
Visa Transactions			MasterCard Transactions		
E-commerce	Non e-commerce	Total	E-commerce	Non e-commerce	Total

The first transaction volume to consider is the e-commerce volume for the higher brand. If the e-commerce transaction volume is between 20,000 and 1 million (regardless of the number of total transactions), the participant is considered a level 3 merchant.

The second transaction volume to consider is the total number of transactions for the higher brand. If the participant is not considered a level 3 merchant by virtue of having at least 20,000 e-commerce transactions, and the total number of transactions is less than 1 million transactions, the participant is considered a level 4 merchant.

The threshold for moving from merchant level 3 to merchant level 2 is one million total transactions of the higher card brand (e.g., Visa). From the perspective of validation requirements (i.e., annual SAQ and quarterly external vulnerability scanning), there is no difference between being a level 3 and level 4 merchant.

5. Identifying the Cardholder Data Environment

The steps to follow to validate PCI compliance, and the complexity of complying, will depend upon the cardholder data environment (CDE). The scope of PCI pertains to any system that either, "processes," "transmits," or "stores" cardholder data. This could be in-house systems or systems outsourced to a service provider. Therefore, it is necessary to perform a complete inventory of where and how merchant cards are accepted for payment.

The State's merchant card provider (STMS) has assigned each participant (considered a legal entity) a "primary" merchant ID (MID), sometimes referred to as a "head chain MID" or a "chain-chain number." Under the primary MID, there is 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.

In the case of an outsourced arrangement with a service provider, the provider is considered part of the CDE. The owner of the primary MID and associated outlet MIDs is considered the merchant of record (MOR), which in most cases is the participant.

However, even if the service provider is the MOR, the entity making the sale or providing the service is consider the "merchant" under the PCI-DSS and is responsible for complying with

certain elements of the standard. The PCI Security Council's definition of a merchant is: *"For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services."*

If the service provider is considered the MOR, the merchant being provided the service (seller of product or service) is considered a "sub-merchant." Both entities are responsible for being PCI DSS compliant.

A) E-commerce Versus Non e-commerce

At the highest level, the two main categories of cardholder data environment (CDE) are: e-commerce and non-e-commerce.

Cardholder Data Environment (CDE) for the Participant's Chain			
Non e-commerce Outlet MIDs (Face-to-face and MOTO capture)		**E-commerce Outlet MIDs** (Website capture)	
In-house	Out-sourced	In-house	Out-sourced

(MOTO = Mail Order Telephone Order)

The appropriate Self-Assessment Questionnaire (SAQ) selected will be based upon the CDE and capture methods. (See Section 16 below.)

B) External Facing IP Addresses

Outlet MIDs that are associated with external (public) facing IP addresses must be identified, as the IP addresses are subject to undergoing external vulnerability scanning performed quarterly by an approved scanning vendor (ASV). See Section 14 below for ASV options. Firewall and network segmentation configurations must be taken into consideration when determining which IP addresses are in scope.

Servers for capture solutions connected via the internet, including VOIP and PCs being used as a virtual terminal, should be included. Capture of a cardholder data in the case of a virtual terminal application can be either keyed via the PC's keyboard or via a magstripe device connected to the PC. In most cases, web solutions that involve an "URL redirect" are not subject to external vulnerability scanning. However, connected web servers facilitating redirects are in PCI scope for other PCI requirements (e.g., anti-virus updates, etc.). POS terminals connected via an analog telephone line are not subject to scanning.

Outlet MIDs Associated with External-Facing IP Addresses			
In-House Hosted Web	Virtual Terminal (Key or swiped)	POS Terminal Connected to IP	POS Software Connected to IP

6. Identifying Third-Party Service Providers

Outsourcing merchant card processing to third-party service providers can limit the scope of PCI compliance, but not eliminate it. The PCI Security Council defines a service provider as any "*business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data."* A service provider would therefore include any company providing a gateway service, a data storage service, or a web hosting service. The merchant's responsibilities pertaining to service providers are identified by Requirements 12.8 and 12.9 of the PCI DSS.

The merchant's responsibilities regarding a service provider are to: 1) maintain a list of service providers; 2) ensure that the provider is compliant by performing a due diligence evaluation prior to engagement; 3) ensure the provider's continued status of compliance by having established an ongoing monitoring process; and 4) have in place a written agreement that identifies the provider's responsibilities regarding compliance roles.

Requirement 12.9 of the standard requires the service provider to acknowledge in writing its responsibility for PCI compliance. A "matrix of responsibilities" document is required, to identify (clarify) the responsibilities of each the participant and the service provider (Requirement 12.8.5).

South Carolina Interactive, LLC (SCI), now branded as NIC-South Carolina , the State's web portal provider (SC.Gov), is considered a service provider. Touchnet used by universities is an example of a service provider. As a provider of various payment gateways (PayPoint, Payeezy, CardConnect), STMS is considered a service provider.

A) Levels of Service Providers

The card brands classify service providers according to two levels, just as merchants are classified into four levels. While both levels are required to complete a SAQ and to undergo external vulnerability scanning, only level 1 service providers are required to undergo an onsite security assessment by a qualified security assessor (QSA). The participant should identify which level each of its service providers is classified.

Participant's Third Party Service Providers	
Level 1	**Level 2**
Processes more than 300,000 transactions annually	Processes less than 300,000 transactions annually
Service provider is required to undergo an onsite security assessment by a QSA	Service provider is not required to undergo an onsite security assessment by a QSA

The participant should determine who within the organization has the responsibility of performing the due diligence and monitoring process, and the frequency. To assist merchants

in their due diligence process of determining and monitoring PCI compliance of a service provider, Visa and MasterCard both maintain a global registry of services providers that have registered with them. The registries can be viewed at: http://www.visa.com/splisting/ and https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html.

A level 2 service provider may not necessarily be registered with Visa, in which case the merchant should secure evidence of compliance directly from the provider. If the service provider is a Level 1 service provider, the provider should be able to furnish evidence of its "Report on Compliance" (ROC).

B) Written Agreement with Service Providers

The participant should inspect its engagement contract with each service provider to ensure it contains the appropriate language to comply with Requirements 12.8 and 12.9 of the standard. If the contract does not (e.g., for older contracts), it is recommended that an addendum be prepared and executed to incorporate the new requirement, including a "matrix of responsibilities."

Although the standard does not require the written agreement to specify the liability of the service provider in the event of a security breach, it is best practice to address the issue. The lack of specificity of liability in the case of a security breach could leave the participant at risk regarding the potential paying of fines assessed by the card brands.

C) Participant Functioning as a Service Provider

There may be cases where the participant may possibly be deemed to be functioning as a service provider. This could be the case where a third-party vendor utilizes the participant's network to process merchant card transactions. Examples of such entities could include an outsourced food service vendor (e.g., Aramark), occasional entertainers (e.g., Harlem Globetrotters), or a legally separate entity but considered a component of the participant (e.g., certain bookstore arrangements). It is possible for such arrangements to be structured such that the participant is only contractually agreeing to provide the entity "web access only service," thereby limiting the participant's PCI-DSS exposure.

D) Internal Service Providers

Consultation with the State's Division of Technology Office (DTO) may be necessary if DTO hosts servers utilized by the participant. DTO could be considered an internal service provider. In some cases, another governmental entity could be an internal service provider. Who manages the servers determines who is responsible for having the servers undergo external vulnerability scanning on behalf of the merchant.

7. Identifying Card Capture Devices

Card data capture devices are of various types, including point of sale (POS) terminals with either swipe devices or keypads. All terminals and devices must be PCI compliant.

Requirement 9.9 of the standard addresses the physical protection of devices that capture payment card data. The purpose is to protect both tampering and substitution of the devices. While the requirement is mandatory for swipe devices, it is recommended for key devices, such as computer keyboards and POS keypads.

The requirement specifically requires the merchant to: 1) maintain an updated list of devices; 2) periodically inspect device surfaces to detect tampering or substitution; and 3) provide training to employees to be aware of attempted tampering or substitution.

The participant should institute procedures to periodically physically inspect for fraudulent skimmers that may be attached to devices, and to check for fraudulent substitution by checking the serial numbers of the devices. Training of employees should include the requirements to: 1) verify the identity of any third-party persons claiming to be repair or maintenance personnel; and 2) be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

The first step in complying with Requirement 9.9 is for the participant to prepare an inventory of all devices, including those in both production and storage.

Card Capture Devices			
Location	Device	Serial Number	Associated Outlet MID

8. Identifying POS Software Applications

Associated with PCI DSS is a separate standard referred to as the Payment Application Data Security Standard (PA-DSS) which requires a merchant to only use validated payment applications. A validated payment application is one that facilitates and does not prevent PCI DSS compliance.

Examples of how an application may prevent PCI DSS compliance include: 1) leaving track data and/or equivalent data on the customer's network after authorization; 2) requiring customers to disable features like anti-virus software or firewalls; and 3) using an unsecured method to connect to the application to provide support to the customer. The list of validated payment applications can be found on the PCI Security Council's Website: https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

After identifying the various payment applications utilized, the participant should: 1) ensure the payment application is listed on the PCI Security Council's Website; 2) ensure the version utilized is consistent with the current version indicated on the Council's Website; and 3) ensure the application is configured correctly.

Note that the PA-DSS does not apply to customized applications developed solely for the participant and not sold or licensed to other third parties. Such applications will not be listed on Visa's Website. However, such customized developed applications may be subject to application penetration testing requirement of PCI DSS. (Requirement 11.3)

POS Software Applications			
Location	Application	Version	Associated Outlet MID

9. Developing a Security Policy for Dissemination

Requirement 12.1 requires the merchant to establish, publish, maintain, and disseminate a security policy. A strong security policy sets the security tone for everyone and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the participant's facilities or otherwise have access to the cardholder data environment. The policy also extends to volunteers.

The policy that is disseminated does not necessarily have to include all the procedures that are to be followed to ensure compliance. It should however contain the expectations of the personnel.

10. Developing an Employee Awareness Training Program

Requirement 12.6 of the standard requires merchants to implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. Employees are to be educated upon hire and must attend refresher training annually. The program must include methodology to allow management to verify and document that employees have completed the training.

The standard also requires each employee to acknowledge at least annually, either in writing or electronically, that they have read and understood the security policy and procedures.

Training should be provided to all personnel that handle and/or process cardholder data. This includes those that: 1) process payments or issue refunds; 2) oversees, manages, or works with card processing software or hardware; 3) manages third-party service providers; and 4) supervises such personnel.

The program developed will depend upon the complexity of the various card capture solutions deployed, as well as the number of employees involved in merchant card processing. Training courses could be developed for different levels of employee roles.

There are two basic options a participant may choose to meet the training requirement: 1) Develop a training program in-house (Power Point materials are available from STO); or 2) utilize the "PCI Data Security Awareness Training" (PCI DSAT) course available to State agencies through SCEIS Central, under "My SCLearning" (developed by STO).

11. Developing a Security Incident Plan

Requirement 12.10 of the standard requires the creation of a security incident response plan in the case of a breach.

A) Requirements of a Security Incident Plan

The standard specifies the items to be included in the plan. Included in the list of items required, the plan should address: 1) the roles, responsibilities, and communication and contract strategies in the event of a compromise including notification of the payment brands; 2) an analysis of legal requirements for reporting compromises; and 3) reference or inclusion of incident response procedures from the payment brands. The standard also requires the annual testing of the plan.

The existence of a general IT incident response plan may not be sufficient, as such plans do not normally incorporate requirements of the payment brands and are sometimes in conflict with the payment brands requirements. It may be appropriate to have a separate plan for PCI compliance, or develop a supplement to the general IT incident response plan. Having a separate plan for PCI facilitates the annual testing of the plan.

Requirements of the payment brands can be viewed at:

http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

B) Timely Security Breach Notifications

Experts indicate that one thing worse than a security breach is not reporting it timely. Failure to make the required notifications timely can increase the potential of fines levied by the card brands, as well as the amount of the fines. Delayed notification can also draw public criticism.

STMS's Operating Procedures require that all security incidents be reported to STMS/Fiserv's fraud department, which will in turn make the appropriate reporting to the card brands. The State Treasurer's policy requires that all reporting be coordinated through STO, not directly with the card brands.

Visa's requirements are that a suspected or confirmed breach be reported immediately. Within 48 hours of Visa being notified, the merchant is to provide evidence of its compliance with PCI DSS. Such compliance evidence will normally include a copy of the latest executed SAQ and results of recent external vulnerability scans, if applicable. Within three business days, the merchant is expected to perform an initial investigation and provide written documentation of any findings or conclusions.

Depending upon the nature of the breach, the brands may require the retaining of an independent PCI forensic investigator (PFI). The card brands must approve the selection of the participant's desired vendor.

It should be noted that most breaches are detected first by the card brands, and the merchant has no prior knowledge of the breach. This is because the brands are usually the first to learn that the breached participant is the common source of stolen card numbers associated with fraudulent transactions.

12. Assessing the Twelve Areas of PCI DSS

The guidance above primarily addresses the requirements that pertain to the business users. There are more complex requirements that pertain to IT staff responsibilities and IT systems. Examples of requirements include encryption of data, firewall and router configuration, network segmentation, log monitoring, software updates, internal and external penetration testing, internal and external vulnerability scanning, etc.

The specific requirements, which are grouped into twelve categories, must be examined to identify the steps required to comply. It is suggested that the participant's PCI Oversight Committee examine each requirement and identify who (business staff or IT staff) will take ownership in seeing that the requirement is addressed. Some of the requirements will be entirely IT related, some entirely business related, and some shared. There will be some requirements that are not applicable to the participant's cardholder data environment.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Depending upon the complexity of the participant's merchant card processing, a participant may deem it appropriate to secure the services of a Qualified Security Assessor (QSA) to assist in addressing the requirements identified in the twelve PCI DSS categories. See Section 14 below regarding options for selecting a QSA.

13. Determining Penetration Testing and Internal Vulnerability Scanning Requirements

If network segmentation is involved, Requirement 11.3.4 is applicable. The section requires annual external and internal penetration tests to validate that segmentation methods are "operational and effective." Penetration tests are different than vulnerability scans (Requirement 11.2). Penetration tests involve advanced hacker techniques to bypass security controls. Penetration testing is generally associated with capture methods associated with SAQs A-EP, C, and D. See PCI Security Council guidance document: https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

Since penetration testing is not applicable to all participants, it will be necessary to ascertain if the requirement applies to the participant's cardholder environment. If it does apply, a determination must be made to see if the participant's staff has the capability and resources to perform the internal and external penetration testing. Otherwise the service may need to be outsourced. If penetration testing is performed by in-house staff, the persons must by qualified staff members who are organizationally independent from those responsible for the security of the systems. Consultation with a QSA is advisable.

14. Validating Compliance via Clover Security

Validating compliance with PCI DSS entails: 1) Preparing the appropriate Self-Assessment Questionnaire (SAQ) on an annual basis (applies to all participants); and 2) Undergoing quarterly external vulnerability scanning of external (public) facing IP addresses, performed by an Approved Scanning Vendor (applies to card capture solutions that involve connecting to the internet). The completing of an SAQ is generally required within 90 days of a merchant implementing a merchant card program. All SAQs have an annual expiration date.

The State Treasurer issued a PCI Data Security Compliance Policy in July 2016, requiring all participants to adhere to the standard. The policy is a reinforcement of a requirement contained in the Participant Agreement the entity executed when it enrolled in the STMS contract. A supplemental policy issued in February 2020 specifies the participant's required process for attesting PCI compliance, as well specifying STO's process for assisting STMS in the monitoring process. The supplemental policy specifies timeframes required to comply and remediation requirements in case of non-compliance.

To accommodate the general policy's requirement to subscribe to a PCI Compliance Validation Service (CVS), and to allow uniform tracking of all participants' compliance status, each participant must be enrolled in STMS's "Clover Security," previously known as PCI Rapid Comply. Enrollment in the portal is under the participant's assigned primary MID, to which all outlet MIDs are associated. After enrollment and completion of its profile, the participant can complete the required SAQ and report its compliance status using the portal's online attestation tool.

Optionally, some participants utilize a qualified security assessor (QSA) to assist in their validation process. QSAs normally use one of two methods in this process. They either:

- Assist the participant in submitting the SAQ through the attestation tool; or
- Prepare a paper "Attestation of Compliance" (AOC) to submit to STMS on the merchant's behalf

Registration in Clover Security is required in either case. In case of the latter, the participant or the QSA must submit the AOC and appropriate SAQ using the following email address: PCI_Compliance@firstdata.com . For compliance documentation submitted via email, the participant's compliance status is denoted in the portal with a placeholder notation.

For entities utilizing NIC-South Carolina (NIC-SC) as their service provider, there are two possibilities regarding PCI DSS compliance responsibility:

- For all State entities whose custodian of their funds is the State Treasurer, the entity is the merchant of record (MOR). The entity, as a participant in the STMS Agreement, is responsible for attesting its PCI DSS compliance as specified herein.
- For entities whose custodian is not the State Treasurer (including quasi-State agencies), NIC-SC is the MOR and the entity is a "sub-merchant." The entity is responsible for attesting its PCI DSS compliance as may be prescribed by NIC-SC for sub-merchants, as the entity is not a participant in the STMS contract.

Any entity whose custodian is not the State Treasurer but processes cards directly with STMS (without utilizing NIC-SC) is responsible for attesting its PCI compliance as specified herein.

STMS keeps STO informed of the current status of all participants as reported through the Clover Security portal. Any participant with a status of non-compliance is subject to the rectification actions specified in the PCI Compliance Supplemental Policy.

New Version of Clover Security

In May of 2020, STMS informed all participants that it was enhancing its PCI Compliance portal by migrating the service's platform to a new vendor. The old platform was provided by Trustwave, and the new platform is being provided by Sysnet Global Solutions.

All participants are now required to be registered under the new Sysnet platform, as all new MIDs have been assigned and the Trustwave platform is no longer available. A "Welcome Email" was sent to each existing participant by STMS when its new primary MID was activated. For those participants who had a status of "compliant" in the old Trustwave portal, that status was carried forward to the new Sysnet portal. Any vulnerability scanning going forward will be performed by Sysnet instead of Touchnet and will be performed quarterly.

Any new participant will receive a "Welcome Email" from STMS when it is assigned its primary merchant ID (MID. The email will provide the participant with instructions for completing the profile registration in Clover Security.

A benefit of the new Sysnet platform is the availability of an optional service that was not available under the Trustwave platform. The new service is known as "ComplyAlly," which provides personalized assistance over the telephone from a highly qualified ComplyAlly agent that understanding the questions asked in the SAQs.

The subscription fee for this optional service is levied annually. Please refer to the State of South Carolina MERCHANT BANK CARD SERVICES Statewide Term Contract Solicitation Number 5400007106 pricing. See Change Order Number 4 and Schedule N that provides for the new service.

http://webprod.cio.sc.gov/SCContractWeb/contractDetail.do?contractNumber=4400011556&hideReturnButton=false

Information regarding the new platform provided by Sysnet can be found at the following link. https://www.cloversecurity.com/index.html.

Enrollment for new participants can be found at the following link:
https://cloversecurity.com/safemaker/login/

STO's supplemental PCI Compliance Policy also addresses certain requirements that any newly applying participant must meet in order for the STO to sign off on before the applicant is allowed to become a participant under the contract.

- Development of a PCI Data Security Policy (See Section 9 above)
- Development of a Security Incident Plan (See Section 11 above)
- Participation in an Employee PCI Awareness Training Program (See Section 10 above)

STO's two PCI Compliance Policies can be viewed on the State Treasurer's website at:
https://www.treasurer.sc.gov/what-we-do/for-governments/banking/

15. Extensive PCI Related Services

The Clover Security Service available from STMS only provides the basic compliance validation service required of a merchant (SAQ and external vulnerability scanning). More extensive PCI-related services such as compliance assessment services and remediation services normally require the services of a security vendor providing such services, beyond services available under Clover Security

Should a participant determine more extensive PCI compliance services are needed (e.g., gap analysis, remediation, penetration testing, etc.), the participant could procure the services from a vendor having the capability to meet the participant's needs. Statewide or convenience contracts that may be available from State Fiscal Accountability Authority (SFAA) Procurement Services or Division of Information Security (DIS) should be considered.

It is recommended that the vendor selected be designated as a "Qualified Security Assessor" (QSA). Verification of a QSA designation can be found on the PCI Security Council's website:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

16. Explanation of the Eight SAQs

Under version 3.2 of the standard, there are eight SAQs to choose from. The SAQ to complete depends upon the participant's cardholder data environment (CDE) and the card capture methods utilized. Only one SAQ per participant (primary MID) is to be completed. The chart below provides guidance as to which SAQ is applicable.

SAQ	Eligibility Requirements
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels, or to MOTO not outsourced.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises.

	Applicable only to e-commerce channels.
B	Merchants using only: Imprint machines with no electronic cardholder data storage, and/or Standalone, dial-out terminals with no electronic cardholder data storage.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. Not applicable to e-commerce.
P2PE	Merchants using approved point-to-point encryption (P2PE) devices, with no electronic card data storage. Not applicable to e-commerce.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.
B	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce merchants.
D	All merchants not included entirely in descriptions for any one of the above SAQ types.
Generally, if multiple payment channels are utilized, SAQ-D must be completed.	

Once enrolled in Clover Security (previously known as PCI Rapid Comply), the tool includes a step-by-step guide in completing the appropriate SAQ. The SAQ is to be completed on an annual basis. Documentation supporting the answers to the SAQ should be maintained. As referenced above, the optional service known as PCI ComplyAlly (specialized telephone assistance in answering the questions) is available.

A participant with multiple channels of card capture (e.g., POS terminals and ecommerce) is normally required to complete SAQ-D. Unless otherwise authorized, attestation of compliance is done at the "primary MID" level.

Multiple Payment Channels

A best-practice technique for a multiple channels situation is to prepare a working draft of the appropriate shorter SAQ for each channel (e.g., POS channel and ecommerce channel). Then when answering the questions online via Clover Security, consider both channels.

Multiple Payment Channels involving both STMS directly and via NIC-SC

A STMS participant for which the State Treasurer is the custodian and that has one payment channel directly with STMS (e.g., POS) and has another payment channel with NIC-SC (e.g., e-commerce), special procedures are required regarding its PCI DSS compliance attestation. This is because the entity has two primary MIDs instead of one. (NIC-SC has its own set of primary MIDs assigned to its partners.)

- Enroll in Clover Security twice, an enrollment for each of the two primary MIDs.
- The MID associated with the STMS-direct payment channel will be considered as the "reporting MID."
- The MID associated with the NIC-SC primary MID will be considered as the "subordinate MID."

- When completing the participant's profile and answering the SAQ questions for the reporting MID, the profile and questions will consider the cardholder data environment for the payment channels associated with both MIDs.
- STMS must be contacted and requested that the subordinate MID be grouped with the reporting MID.

Refer to PCI's most recent document to assist in determining which SAQ to complete:
https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2.pdf

A publication for "Best Practices for Securing E-commerce" can be found at website: https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf?agreement=true&tim

17. Encryption Considerations

The use of solutions available from STMS, including certain Clover devices and TransArmor, providing for point-to-point encryption (P2PE) and tokenization may limit the scope of PCI. Solutions providing end-to-end encryption (E2EE) are available as well.

Use of P2PE solutions generally reduces the number of SAQ questions. Information on P2PE solutions can be viewed at:
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

If only card-present solutions are utilized an accepted P2PE equipment is utilized, the shorter SAQ-P2PE may be utilized.
https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-P2PE.pdf

Participants that only conduct "face-to-face" and "mail order / telephone order" (MOTO) transactions may be eligible to complete the shorter "SAQ B-IP" if certain approved POS certified POS terminals are used. SAQ B-IP is intended for merchants who use PCI PTS-approved point-of-interaction (POI) devices that communicate to the payment processor over an IP-based (Internet Protocol) network. The list of PTS-approved devices can be found at: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Participants should be aware that a new version of the standard (version 4.0) is expected sometime in the future, at which time some POS terminals currently compliant with the standard may not be considered compliant under the new standard. STMS can advise of POS terminals most suitable for reducing PCI scope.