SC State Treasurer's Office
PCI Data Security Compliance Roadmap
July 2016

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). STO entered into a new contract with SunTrust Merchant Card Services (STMS) in 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 new contract with STMS provides for an optional service a participant may subscribe in order to validate its compliance with PCI DSS. The service is referred to as First Data's PCI Rapid Comply® and is addressed herein.

This document provides <u>suggested</u> 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 with PCI DSS
- Extensive PCI related services
- Explanation of the eight SAQs

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 be required to prepare, either through PCI Rapid Comply® or otherwise.

1. **Source of Compliance Requirements**

   Compliance with PCI DSS is a <u>contractual requirement</u> of the merchant card service provider (acquirer bank) from which card processing services are obtained. The contract with the State's merchant card servicer [SunTrust Merchant Services / First Data (STMS)] requires compliance with the card brands rules, which allude to potential fines for noncompliance of PCI. The standard, which is subject to revisions from time to time, is promulgated by the PCI Data Security Council, which was established by the card brands.

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 – Reporting the validation of compliance whenever requested by either STMS or the card brands. Attestation often times requires documentation supporting the validation tasks

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 will require extensive support from IT. Thus, PCI DSS compliance is primarily deemed to be a <u>business problem</u> with an <u>IT solution</u>.

   Because many of the PCI compliance and validation requirements involve IT solutions, in the past some participants have tended to rely upon their IT departments to assume the entire responsibility of compliance. However, many of the PCI <u>compliance tasks</u> involve the business users as well. Therefore, the compliance component of the process is a joint responsibility of both the business and IT sectors. 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.

   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.

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 levels is that of the "doing business as" (DBA) entity, which in most cases is the participant's single chain level, not individual merchant number levels or departments. Under the State's master contract, STMS/First Data monitor's each participant's transaction total volume and e-commerce volume and makes the official determination of the merchant'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, and 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 level 3 to 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, can vary from participant to participant. 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 processor (STMS) has assigned each participant a "chain number." Under the chain, there are generally multiple "merchants" (also referred to as "outlets"). For a large participant (e.g., university) there could be more than a dozen merchant numbers. The participant's merchant numbers associated with its chain number can be viewed through the merchant card processor's online reporting tool (i.e., ClientLine).

In the case of an outsourced arrangement with a service provider, the owner of the merchant number depends upon who is functioning as the "merchant," the participant or the service provider. In either case, the capture solution should be identified as part of the participant's cardholder data environment (CDE).

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 Merchant Numbers (Face-to-face and MOTO capture)		E-commerce Merchant Numbers (Website capture)	
In-house	Out-sourced	In-house	Out-sourced

The appropriate Self-Assessment Questionnaire (SAQ) selected will be based upon the CDE and capture methods. (See discussion on Self-Assessment Questionnaires - page 13 below.)

B) External Facing IP Addresses

Merchant numbers that are associated with external (public) facing IP addresses must be identified, as the IP addresses are subjected to undergoing external vulnerability scanning. Firewall and network segmentation configurations must be taken into consideration when determining which IP addresses are in scope.

In most cases, merchant numbers for web solutions that involve an "URL redirect" are not subject to external vulnerability scanning and should not be included below. Additionally, POS terminals connected via an analog telephone line should not be included. Terminals connected via the internet, including VOIP, should be included.

Merchant Numbers Associated with External-Facing IP Addresses			
In-House Hosted Web	Virtual Terminal	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 in sections 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.

A new requirement of version 3.2 of the standard (section 12.9) requires the service provider to acknowledge in writing to the merchant its responsibility for PCI. This requirement became effective July 1, 2015.

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 <u>more</u> than 300,000 transactions annually	Processes <u>less</u> than 300,000 transactions annually
Service provider is <u>required</u> to undergo an onsite security assessment by a QSA	Service provider is <u>not</u> required to undergo an onsite security assessment by a QSA

The participant should determine who within the agency/university 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 section 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.

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.

Participants utilizing South Carolina Business One Stop (SC BOS) should consider SC BOS as a service provider. Participants utilizing South Carolina Interactive, LLC, (SCI) where card payments are processed under the STMS/STO contract, should consider SC Interactive as a service provider.

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 campus's PCI exposure. Consultation with a QSA is advised.

Agreements with these entities should address the PCI responsibility of each party. Depending upon the arrangement, the participant could be functioning as a service provider while the third-party may be functioning as a merchant. A participant deemed to be functioning as a service provider may be subject to completing SAQ D-SP, as well as section 12.9, which requires the participant to acknowledge in writing that the participant is considered PCI compliant as a service provider.

7. **Identifying Card Capture Devices**

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

Additionally, a new requirement in version 3.2 of the standard (section 9.9) 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.

Section 9.9 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: 1) to 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 Section 9.9 is for the participant to prepare an inventory of all devices campus-wide. Note that this requirement became effective July 1, 2015.

Card Capture Devices			
Location	Device	Serial Number	Associated Merchant Number

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. (Section 11.3)

POS Software Applications			
Location	Application	Version	Associated Merchant Number(s)

9. Developing a Security Policy for Dissemination

Section 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 necessary 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

Section 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; and 3) supervises such personnel.

The program a participant develops 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 entirely in-house; or 2) Utilize a third-party vendor that provides an online training service.

A participant with a limited number of employees involved with the processing of merchant cards may elect to develop an in-house training program. This option may be pursued if the number of employees is manageable, a training module is available, and a proper tracking and documentation process is in place.

Third-party vendors that provide online training and employee tracking generally provide a subscription service, with its fees being based upon the number of subscribers (seats). A participant may select any vendor of its choice to provide online training.

11. Developing a Security Incident Plan

Section 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 <u>general</u> 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 <u>separate</u> 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) <u>Timely Security Breach Notifications</u>

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 requires that all security incidents be reported to STMS, which will be addressed by the fraud department.

Visa's requirements are that a suspected or confirmed breach be reported immediately. Within <u>48 hours</u> of notifying Visa, the merchant is to provide <u>evidence</u> 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 <u>three business days</u>, 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. A participant may select any vendor of its choice to provide QSA assessment and support services.

13. Determining Penetration Testing and Internal Vulnerability Scanning Requirements

A new requirement in version 3.2 of the standard (section 11.3.4) requires annual external and internal penetration tests to validate that segmentation methods are "operational and effective." Penetration tests are different than vulnerability scans (section 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 with PCI DSS

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).

STMS generally requires annual <u>attestation</u> of the validation of PCI compliance. Failure to attest compliance with PCI DSS when requested could potentially result in suspension of card processing services from STMS. Additionally, should a security breach occur, the card brands will be requiring <u>proof</u> of PCI DSS compliance at the time of the breach.

Participants considered level 3 or level 4 merchants have two options to <u>validate</u> PCI compliance: 1) Contract with a Qualified Security Assessor (QSA) to perform the two required tasks; or 2) Subscribe to First Data's PCI Rapid Comply® Service (provided at no charge by STMS. Participants considered level 1 and 2 merchants must utilize a qualified security assessor (QSA) to perform it validation tasks.

If PCI Rapid Comply® Service is desired, online enrollment is available. Refer to Schedule E of the STMS/STO contract, and to information available on First Data's website: https://www.pcirapidcomply.com/faq.html

15. Extensive PCI Related Services

Previously, the STO had a master contract with Trustwave, under which agencies could acquire PCI validation services, as well as optional extensive PCI services. With the PCI Rapid Comply® service becoming available to agencies (at no cost) under the 2015 STMS merchant card services contract, the STO master contract with Trustwave is no longer an option for agencies.

Note that PCI Rapid Comply® available from STMS only provides the <u>basic</u> compliance validation service required of a merchant (SAQ and external vulnerability scanning).

More extensive PCI-related services, such as internal vulnerability scanning, internal penetration testing, external penetration testing, compliance assessment services, and remediation services, normally require the services of a security vendor providing such services, beyond services available under PCI Rapid Comply®.

Should a participant determine that the PCI Rapid Comply® Service is not sufficient for its unique needs, the participant could procure some or all its PCI related services from a vendor that has the capability to meet the agency's needs. Any statewide or convenience contract that may be available from the Materials Management Office (MMO) or Division of Information Security (DIS) should be considered.

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. The chart below provides guidance as to which SAQ is applicable.

Face-to-Face and MOTO Only		E-Commerce Only	
B	POS analog not connected to IP *	A	Card-not-present fully outsourced *
B-IP	POS connected to IP * #	A-EP	Outsourced, but website redirect can impact security of payment * # &
C-VT	Virtual Terminal IP, dedicated or segmented, and keyed only * #		
C	POS Software connected to IP, dedicated or segmented * # &		
P2PE-HW	POS hardware managed w/ Point to Point Encryption *		
D	Cardholder data is stored # &	D	Cardholder data is either processed, transmitted, or stored # &
Combination of Face-to-Face and E-Commerce			
D	All merchants not included <u>entirely</u> in any <u>one</u> of the above, or where cardholder data is stored (Systems are connected / Not segmented) # &		

* Cardholder data not stored; **#** Vulnerability scanning required; **&** Pen test potential

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
The PCI Rapid Comply® solution includes a guided, step-by-step SAQ tool help.

The SAQ is to be completed on an annual basis. Documentation supporting the answers to the SAQ should be maintained. If remediation is required in order to become compliant, the creation of a remediation plan is recommended, and may be required by STMS.

Although the completion of an SAQ may be delegated, the signature contained on a SAQ should be that of a responsible individual, normally within the business sector. Should the validity of a SAQ ever be questioned, the person who signed the SAQ will normally be the individual held accountable.

The STMS/First Data PCI Compliance Department may occasionally request attestation of the completion of the SAQ, and may request evidence of the successful results of the most recent external vulnerability scans, if applicable. The prompt reply to all compliance requests should be made.

The use of First Data's TransArmor solution, providing for point-to-point encryption and tokenization, may limit the scope of PCI, allowing for positive response to some of the questions on the SAQs.