Merchant Card Enrollment Guidance SC Office of the State Treasurer – Banking Division Updated August 2023

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 Treasurer has a contract with a merchant card provider to service all State entities. The contract, known as the Payment Solutions Agreement, is with Fiserv's "First Data Merchant Services, LLC" (FDMS). Information regarding the contract is found below.

There are two category 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 FDMS or through SC.Gov, a web portal service provided by Tyler Technologies. 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. All payment gateway providers must be able to process merchant card transactions through FDMS.

State Treasurer's Merchant Card Contract (Payment Solutions Agreement)

Information about the State Treasurer's contract with FDMS can be found at the following link: https://treasurer.sc.gov/resources/banking-forms-and-policies/payment-solutions-agreement/

To participate in the contract, an entity is required to execute the appropriate "Services Participation Agreement". It is critical that the entity read all components of the contract, as execution of the Services 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 <u>all</u> participants are:

- Payment Solutions Agreement
- Schedule A Services Subscribed to by Participant
- Schedule B Schedule of Fees
- Schedule C Point of Sale "POS" Terminals
- Schedule D PCI Rapid Comply (Clover Security) 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 <u>optional</u> basis and without an additional procurement process:

- First Data Merchant Services (FDMS) for merchant card processing
 - o PayPoint
 - o Payeezy
 - o CardConnect
- Tyler Technologies 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:

- Tyler Technologies's SC.Gov For both ecommerce and POS transactions
- Touchnet PayPath For universities***
- FDMS's Managed Service Fee For use with PayPoint, CardConnect, or Payeezy payment gateways

***Any vendor offering a payment gateway must be able to process merchant card transactions through FDMS.

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 with Tyler Technologies for Digital Government Services is administered by the Department of Administration's Division of Technology. Information regarding the contract can be found at the following links:

https://procurement.sc.gov/contracts/search?v=17613-9918-0-0

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:

Merchant Card Enrollment Guidance – Updated August 2023

- Compliance is a contractual obligation to FDMS
- Failure to comply with the standard may result in substantial fines levied by the card brands
- Attestation of compliance through FDMS's PCI Rapid Comply (Clover Security) portal is required
- FDMS 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/resources/banking-forms-and-policies/

https://www.clover.com/small-business-resources/pci-compliance

Merchant IDs (MIDS)

Once enrolled, a participant (considered a legal entity) will be assigned a "primary" merchant ID (MID), sometimes referred to as 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 FDMS's reporting tool (ClientLine Enterprise). A participant's PCI compliance attestation is done at the primary MID level.

	Enrollment Process - Merchant Card Bank Services Contract				
		Task	Reference / Comment		
1		Review the Payment Solutions Agreement, including terms, optional services offered, and fee schedules	Available on State Treasurer's website. Schedule A lists all services. Schedule B list the service fees. Schedule C list the equipment fees. Schedule D is for the PCI Rapid Comply (Clover Security) Service. Other schedules pertain to optional services.		
2		Review STO's policies and documents pertaining to PCI Compliance	Available at the links above. PCI compliance is a prerequisite for participation in the Payment Solutions Agreement with FDMS.		
3		Consult with FDMS regarding card capture options and/or payment gateways	Obtain from FDMS recommendations for equipment, capture devices and payment gateways. Engage Tyler Technologies in the discussions if SC.Gov will be utilized.		
4	а	Take three initial steps for PCI compliance	Three action items are required prior to STO executing the Services Participation Agreement. Develop a: PCI Compliance policy; Security Incident Plan; and Employee Awareness Training.		
	b	Advise STO of 3 actions taken	Submit evidence to STO prior to or along with the Services Participation Agreement.		
5	а	Execute and submit the appropriate Services Participation Agreement (SPA)	The SPA can be found at: https://treasurer.sc.gov/media/82148/exhibit-2.pdf		

b Complete Schedule A – Menu of Services Available sorvices Available subscribe to and attach to the SPA that is to be submitted. c Submit SPA to STO SPA can be submitted via email to STO at STOBankingOperations@sto.sc.gov STO and FDMS executes SPA After verification of the three initial PCI compliance action items, STO will coordinate with FDMS execution of the SPA. 7 a Complete Merchant Outlet Setup Form(s) provided by FDMS. (Provided by FDMS.) (Provided by FDMS. (Provided by FDMS.) (Provided by FDMS.				
subscribe to and attach to the SPA that is to be submitted. C Submit SPA to STO SPA can be submitted via email to STO at STOBankingOperations@sto.sc.gov After verification of the three initial PCI compliance action items, STO will coordinate with FDMS execution of the SPA. After verification of the three initial PCI compliance action items, STO will coordinate with FDMS execution of the SPA. Complete Merchant Outlet Setup Form(s) provided by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) Settlement bank account, billing information is necessary for FDMS staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.). b Select invoicing option c Determine if Discover and/or Amex will be accepted c Determine if Discover and/or Amex will be accepted d MasterCard are included in basic service. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. B Determine capture devices for card-present transactions C C Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available from a additional fee per transaction (See Schedule B of Payment Solutions Agreement). D Determine gateway needed for card-absent transactions b Install & test devices/software D Determine gateway needed for card-absent transactions b Install & test devices/software D Determine gateway needed for card-absent transactions D Signate PCI Compliance Point of Contact D Esignate PCI Compliance Point of Contact D Esignation PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. Supplemental policy. Advise and keep STO updated of POC. Supplement is normally done by the PCI POC. If a QSA is involved, the participant c		b	-	
Submit SPA to STO			of Services Available	
STOBankingOperations@sto.sc.gov		С	Submit SPA to STO	
STO and FDMS executes SPA After verification of the three initial PCI compliance action items, STO will coordinate with FDMS execution of the SPA. Complete Merchant Outlet Setup Form(s) provided by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) by Select invoicing option by Select invoicing option complete a separate form for each outlet (line of business or location) to be established. Information is necessary for FDMS staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.). by Select invoicing option by Select invoicing option complete a separate form for each outlet (line of business or location) to be established. Information is necessary for FDMS staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.). Invoicing can be at primary MID level (central billing) or at each outlet level. If Tyler Technologies is utilized, Tyler Technologies is utilized, Tyler Technologies and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. by Chip-enabled POS Terminals repaired by software. POS terminals are available from FDMS. POS software may be obtained elsewhere. complete a separate form for each outlet (line of business or lost stops and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. by Chip-enabled POS Terminals repaired sevents and Amex each requires separate registration. Amex also requires separate registration.				
items, STO will coordinate with FDMS execution of the SPA. Complete Merchant Outlet Setup Form(s) provided by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) Select invoicing option b Select invoicing option c Determine if Discover and/or Amex will be accepted c Determine if Discover and/or Amex will be accepted c Determine capture devices for card-present transactions b Chip-enabled POS Terminals c Encryption (E2E or P2PE)? Determine gateway needed for card-absent transactions D Determine capture devices/software D Determine capture devices/software D Determine capture devices for card-present transactions Recommended D Determine capture devices for card				
Complete Merchant Outlet Setup Form(s) provided by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) Staff to established. Information is necessary for FDMS FDMS. (Provided by Tyler Technologies if SC.Gov is involved) Staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.).	6		STO and FDMS executes SPA	After verification of the three initial PCI compliance action
Setup Form(s) provided by FDMS. (Provided by Tyler Technologies if SC.Gov is involved) b Select invoicing option c Determine if Discover and/or Amex will be accepted a Determine capture devices for card-present transactions b Chip-enabled POS Terminals c Encryption (E2E or P2PE)? D Determine gateway needed for card-absent transactions a Procure devices/software b Install & test devices/software D Designate PCI Compliance Point of Contact 12 Create a PCI Oversight (Committee (Best Practice) (Chain level) D Enroll IP addresses to be Lincologies is contact the STO at STOBanking Operations (Post Stermens) are available from STO. Supplemental policy. Advise and keep STO updated of POC. If a QSA is involved. D Enroll IP addresses to be Location) to be established. Information is necessary for FDMS staff to establish the appropriate setups on various systems (Merchant numbers, Clientline Enterprise, Capture Method, Settlement bank account, billing information, staff the establish the appropriate setups on various systems (Merchant numbers, Clientline Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.). Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain sevel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing can be at primary MID level (cachain evel.) Invoicing catch.) Invoicing can be at primary MID level (cachain evel.) Invoicing catch.) Invoi				items, STO will coordinate with FDMS execution of the SPA.
FDMS. (Provided by Tyler Technologies if SC.Gov is involved) staff to establish the appropriate setups on various systems (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement bank account, billing information, statement rendering, etc.). b Select invoicing option c Determine if Discover and/or Amex will be accepted d Determine capture devices for card-present transactions b Chip-enabled POS Terminals c Encryption (E2E or P2PE)? Determine gateway needed for card-absent transactions d Procure devices/software b Install & test devices/software b Install & test devices/software b Install & test devices/software c Determine gateway needed for card-absent transactions b Install & test devices/software c Determine gateway needed for card-absent transactions d Procure devices/software d Possignate PCI Compliance Point of Contact D Designate PCI Compliance Point of Contact D Designate PCI Compliance Point of Contact D Designation of PCI Compliance POC is required by service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be staff to establish the appropriate setups on various by the PCI POC. If a QSA is involved. staff to establish the appropriate setups. Capture Method, Settlement pendering, etc.) (Merchant numbers, ClientLine Enterprise, Capture Method, Settlement pendering, etc.) Invoicing can be at primary MID level (chain level) staff to establish the appropriate Sourcunt, billing information, statement rendering, etc.). Invoicing can be at primary MID level (chain level) staff to establish the appropriate Solling information, statement reach outlet level. If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. From FDMS or software vendor, and in some cases from Tyler Technologies Designation of PCI Compliance POC is required by Designation of PCI Compliance POC is required by Source vendor of PCI Compliance POC is required by Source vendor of PCI Compliance is re	7	а	Complete Merchant Outlet	Complete a separate form for <u>each</u> outlet (line of business or
Technologies if SC.Gov is involved) Settlement bank account, billing information, statement rendering, etc.). b Select invoicing option Invoicing can be at primary MID level (central billing) or at each outlet level. If Tyler Technologies is utilized, Tyler Technologies is invoiced. c Determine if Discover and/or Amex will be accepted and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations, soc.gov for more information on the AMEX participation agreement. POS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). Poetermine gateway needed for card-absent transactions If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. Prom FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) 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. 3 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be (Applies if external-facing IP address are involved.				·
involved) Settlement bank account, billing information, statement rendering, etc.). b Select invoicing option Invoicing can be at primary MID level (central billing) or at each outlet level. If Tyler Technologies is utilized, Tyler Technologies is invoiced. C Determine if Discover and/or Amex will be accepted Visa and MasterCard are included in basic service. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. POS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. b Chip-enabled POS Terminals c Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions 10 a Procure devices/software b Install & test devices/software rechnologies b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Applies if external-facing IP address are involved.				
rendering, etc.). b Select invoicing option Invoicing can be at primary MID level (central billing) or at each outlet level. If Tyler Technologies is utilized, Tyler Technologies is invoiced. c Determine if Discover and/or Amex will be accepted Visa and MasterCard are included in basic service. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. POS terminals or software. POS terminals are available from EDMS. POS software may be obtained elsewhere. b Chip-enabled POS Terminals Recommended Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Promation of PCI Compliance POC is required by of Contact 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Within 90 days of implementation. Applies if external-facing IP address are involved.			_	
b Select invoicing option Invoicing can be at primary MID level (central billing) or at each outlet level. If Tyler Technologies is utilized, Tyler Technologies is invoiced. Visa and MasterCard are included in basic service. Discover and Amex will be accepted Amex will be accepted Determine if Discover and/or Amex will be accepted Amex will be accepted Determine capture devices for card-present transactions Determine capture devices for card-present transactions Determine (E2E or P2PE)? Determine gateway needed for card-absent transactions Designate PCI Compliance Point of Contact Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Create a PCI Oversight Committee (Best Practice) Designation of PCI Compliance POC is required by sortion of PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Procure devices/software Designation of PCI Compliance POC is required by sortion of PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Procure devices/software Designation of PCI Compliance POC is required by sortion of PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.			involved)	
each outlet level. If Tyler Technologies is utilized, Tyler Technologies is invoiced. C Determine if Discover and/or Amex will be accepted Amex will be accepted Determine and Master Card are included in basic service. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. Determine capture devices for card-present transactions Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. POS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. POS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. POS terminals or software. POS terminals are available from FDMS. POS software and post post post post transactions are available for a process. Post post post post post post post post p		la la	Calastinosciaina autian	
Technologies is invoiced. C Determine if Discover and/or Amex will be accepted C Determine if Discover and/or Amex will be accepted C Determine if Discover and/or Amex will be accepted C Determine capture devices for card-present transactions C Determine capture devices for card-present transactions C Determine (E2E or P2PE) Province C Determinals or software Post transactions C Determine gateway needed for card-absent transactions D Determine gateway needed for card-absent transactions appropriate SOW directly with Tyler Technologies. D Determine gateway needed for card-absent transactions appropriate SOW directly with Tyler Technologies. D Determine gateway needed for card-absent transaction is sufficiently in the PCI compliance POC is required by supplemental policy. Advise and keep STO updated of POC. D Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. Such committee has the res		D	Select invoicing option	
c Determine if Discover and/or Amex will be accepted Nisa and MasterCard are included in basic service. Discover and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. PoS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. C Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). Determine gateway needed for card-absent transactions Procure devices/software If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. Prom FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Applies if external-facing IP address are involved.				,
Amex will be accepted and Amex each requires separate registration. Amex also requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. 8 a Determine capture devices for card-present transactions POS terminals or software. POS terminals are available from FDMS. POS software may be obtained elsewhere. 8 c Chip-enabled POS Terminals Recommended 9 c Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions appropriate SOW directly with Tyler Technologies. 10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation.		_	Determine if Discover and/or	•
requires signing a separate AMEX participation agreement. Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. B a Determine capture devices for card-present transactions FDMS. POS software. POS terminals are available from FDMS. POS software may be obtained elsewhere. C Chip-enabled POS Terminals Recommended C Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). Determine gateway needed for card-absent transactions Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Done at the primary MID level (chain level) De Enroll IP addresses to be Applies if external-facing IP address are involved.			-	
Please contact the STO at STOBankingOperations@sto.sc.gov for more information on the AMEX participation agreement. 8 a Determine capture devices for card-present transactions FDMS. POS software. POS terminals are available from FDMS. POS software may be obtained elsewhere. b Chip-enabled POS Terminals Recommended c Encryption (E2E or P2PE)? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions 10 a Procure devices/software b Install & test devices/software 11 Designate PCI Compliance Point of Contact 12 Create a PCI Oversight Committee (Best Practice) 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be POS terminals or software. POS terminals are available from FDMS or software was available from saliable from saliable from STO. POS terminals or software. POS terminals are available from EDMS or Software saliable from STO. POS terminals or software. POS terminals are available from saliable from saliable from STO. POS terminals or software. POS terminals are available from saliable from STO. POS terminals or software POS terminals are available from saliable from STO. Validation of PCI compliance Roadmap" document for guidance. Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Agreement. POS terminals of PCI compliance POS is required within 90 days of implementation.			Amex will be decepted	, , ,
for more information on the AMEX participation agreement. B a Determine capture devices for card-present transactions FDMS. POS software. POS terminals are available from FDMS. POS software may be obtained elsewhere. C Chip-enabled POS Terminals Recommended C Encryption (E2E or P2PE)? Determine gateway needed for card-absent transactions Determine gateway needed for card-absent transactions Procure devices/software Designate PCI Compliance Designate PCI Compliance POI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. Create a PCI Oversight Committee (Best Practice) Create a PCI Oversight Committee (Best Practice) Create a PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Designation on the AMEX participation agreement. POS terminals or software. POS terminals are available from spots available				
B a Determine capture devices for card-present transactions FDMS. POS software may be obtained elsewhere.				
b Chip-enabled POS Terminals c Encryption (E2E or P2PE) ? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions 10 a Procure devices/software b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Committee (Best Practice) 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Potermine Recommended Understand PCI implications before selecting. P2PE is available on some additional FCI implications before selecting. P2PE is available for an additional fee per transaction (See Schedule B of Payment Solutions before selecting. P2PE is available for an additional fee per transaction (See Schedule B of Payment Solutions before selecting. P2PE is available for an additional fee per transaction (See Schedule B of Payment Solutions had in additional fee per transaction (See Schedule B of Payment Solutions additional fee per transaction (See Schedule B of Payment Solutions Agreement). If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. From FDMS or software vendor. Prom FDMS or software vendor. Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. 13 a Enrollment in PCI Rapid Comply service (online portal) involved, the participant could request FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation.	8	а	Determine capture devices for	
c Encryption (E2E or P2PE) ? Understand PCI implications before selecting. P2PE is available on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). Determine gateway needed for card-absent transactions Procure devices/software b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Committee (Best Practice) Designation of PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Table Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. From FDMS or software vendor, and in some cases from Tyler Technologies Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Table Technologies Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Table Technologies Assisted by FDMS or by software vendor Designation of PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.			card-present transactions	FDMS. POS software may be obtained elsewhere.
on some devices. TransArmor is available for an additional fee per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. 10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) 13 b Enroll IP addresses to be Applies if external-facing IP address are involved.		b	Chip-enabled POS Terminals	Recommended
per transaction (See Schedule B of Payment Solutions Agreement). 9 Determine gateway needed for card-absent transactions appropriate SOW directly with Tyler Technologies. 10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.		С	Encryption (E2E or P2PE) ?	,
Agreement). 9 Determine gateway needed for card-absent transactions appropriate SOW directly with Tyler Technologies. 10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Applies if external-facing IP address are involved.				
9 Determine gateway needed for card-absent transactions 10 a Procure devices/software 11 Designate PCI Compliance Point of Contact 12 Create a PCI Oversight Committee (Best Practice) 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Instell Bates devices/software If Tyler Technologies is utilized, obtain and execute appropriate SOW directly with Tyler Technologies. From FDMS or software vendor, and in some cases from Tyler Technologies Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.				
card-absent transactions appropriate SOW directly with Tyler Technologies. 10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); UAIdation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.				•
10 a Procure devices/software From FDMS or software vendor, and in some cases from Tyler Technologies b Install & test devices/software Assisted by FDMS or by software vendor 11 Designate PCI Compliance Point of Contact Supplemental policy. Advise and keep STO updated of POC. 12 Create a PCI Oversight Committee (Best Practice) 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. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.	9		<u> </u>	·
Technologies b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Besignate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) Create a PCI Oversight 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. Is a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Technologies Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.	10	_		, , , , , , , , , , , , , , , , , , , ,
b Install & test devices/software Designate PCI Compliance Point of Contact Create a PCI Oversight Committee (Best Practice) a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Install & test devices/software Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Assisted by FDMS or by software vendor Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation.	10	а	Procure devices/software	•
Designate PCI Compliance Point of Contact supplemental policy. Advise and keep STO updated of POC. Create a PCI Oversight Committee (Best Practice) 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. If a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC. 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Designation of PCI Compliance POC is required by supplemental policy. Advise and keep STO updated of POC.		h	Install & tost devises/software	· ·
of Contact Create a PCI Oversight Committee (Best Practice) Buch 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.	11	D	•	
Create a PCI Oversight Committee (Best Practice) 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. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.	**		•	, ,
Committee (Best Practice) actions to comply with the PCI Data Security Standard, using STO's "PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be actions to comply with the PCI Data Security Standard, using STO's "PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.	12			
STO's "PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be STO's "PCI Compliance Roadmap" document for guidance. Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.	**		•	, , , , , , , , , , , , , , , , , , , ,
Sample charter is available from STO. 13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Sample charter is available from STO. Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.			(2000, 1000,00)	
13 a Enrollment in PCI Rapid Comply service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be Validation of PCI 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 FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.				
service (online portal) (AKA Clover Security); Done at the primary MID level (chain level) b Enroll IP addresses to be portal. Enrollment is normally done by the PCI POC. If a QSA is involved, the participant could request FDMS to complete the enrollment on its behalf. Validation of compliance is required within 90 days of implementation. Applies if external-facing IP address are involved.	13	а	Enrollment in PCI Rapid Comply	
Done at the primary MID level (chain level) enrollment on its behalf. Validation of compliance is required within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.				portal. Enrollment is normally done by the PCI POC. If a QSA is
(chain level) within 90 days of implementation. b Enroll IP addresses to be Applies if external-facing IP address are involved.			(AKA Clover Security);	
b Enroll IP addresses to be Applies if external-facing IP address are involved.			• •	
scanned		b		Applies if external-facing IP address are involved.
			scanned	

С	Validate compliance	Enrollment in PCI Rapid Comply (Clover Security) should be
		prior to any card transactions. Validation of compliance (SAQ
		completion) is required within 90 days of implementation.