APPLICABILITY OF PCI DATA SECURITY STANDARD (PCI DSS)
TO CARD CAPTURE METHODS
NC Office of the State Controller

General Requirements for Merchants

- All merchants and their service providers are required to be compliant with the PCI Data Security Standard.
- Merchants must "validate" their compliance, depending upon their assigned Merchant Level (1 – 4)
- As part of the validation process, all merchants must complete an annual Self-Assessment Questionnaire (SAQ), based upon the capture solution they utilize. (Version 1.2 applies. See chart below.)
- For any environment under which un-masked cardholder data is stored electronically, SAQ-D applies.
- For any environment involving external-facing (public) IP addresses (network or web), quarterly vulnerability scanning by an Approve Scanning Vendor (ASV) is required.
- For any environment storing cardholder data electronically (SAQ-D), an annual penetration test is required.
- For any environment using vendor-supplied payment applications, the Payment Application Standard (PA-DSS) applies. (In-house applications developed by merchants or service providers that are not sold to a third party are not subject to the PA-DSS, but subject to PCI DSS.) (Implementation Guide must be provided.)
- Capture applications accepting PIN debit cards must adhere to the PCI Pin Transaction Security (PCI PTS), with the PIN device being on the PCI Council's List of Approved PEDs. (Effective July 1, 2010)
- All participants in the MSA with SunTrust Merchant Services must be enrolled in TrustKeeper in order to facilitate their validation requirements ("SAQ Only," or "SAQ and Vulnerability Scanning")

If a Service Provider (gateway service, data storage service, web hosting company, etc.) is utilized:

- Requirement 12.8 of the PCI DSS applies, which relates to the merchant's responsibility
- Must have a "written agreement" indicating the service provider's responsibility for PCI compliance
- Must perform due diligence before engaging with any new service provider
- Must obtain from the service provider evidence of their PCI compliance and monitor their compliance
- Evidence could be a "Report on Compliance" (ROC), or be listed on Visa's List of Approved Service Providers - List of Compliant Service Providers (in addition to a written agreement).
- A "Level 2" service provider may not have a ROC or be listed on Visa's site and if not, must provide evidence of SAQ-D and scanning (in addition to a "written agreement").
- Requirements for Service Providers are found on Visa's Website.

Use This Chart To Determine Which Requirements Apply to Your Capture Method

Card Capture Method	Required Vulnerability Scanning of IP Addresses	Required Annual Self-Assessment Questionnaire (SAQ)	Compliance w/ Payment Application Standard	Service Provider Subject to PCI DSS
POS Terminal (stand-alone) - Using analog dial up telephone line to transmit data to the acquirer	No. Since no PCs or network servers are involved.	SAQ B if data is not stored in electronic format. SAQ D if not qualified for SAQ B	N/A	N /A
POS Terminal (stand-alone) - Using internet to transmit data to the acquirer	Yes. Since POS terminal is connected to a server that is connected to the Internet	SAQ C if data is not stored in electronic format. SAQ D if not qualified for SAQ C	N/A	N/A
POS Software Application - Using Internet to transmit data to the acquirer	Yes. Since PC the POS software is housed on is connected to the Internet	SAQ C if data is not stored in electronic format; and the POS and Internet connection are on the same device; and POS is not connected to any other system; and the POS	Yes – Off-the-shelf applications must be listed on PCI Security Council's List of Validated Payment Applications; or on	N/A

		vendor uses secure techniques to provide remote support. SAQ D if not qualified for SAQ C	Visa's List of Validated Payment Applications See note above regarding in-house developed or custom built applications	
POS Software Application - Using analog dial up telephone to transmit data to the acquirer	Yes if software is on a PC or network connected to the Internet. No if software in not on a PC or network connected to the Internet.	SAQ C if data is not stored in electronic format; and POS is not connected to any other system; and the POS vendor uses secure techniques to provide remote support. SAQ D if not qualified for SAQ C	Yes - Off-the-shelf applications must be listed on PCI Security Council's List of Validated Payment Applications; or on Visa's List of Validated Payment Applications (See note above regarding in-house developed or custom built applications.)	N/A
Third Party Service Provider – Card data captured by merchant and then transmitted to Provider functioning as a gateway	Yes. Since data is initially processed and transmitted on merchant's server	SAQ C if data is not stored in electronic format; and the application and Internet connection are on the same device; and application is not connected to any other system; and the application vendor uses secure techniques to provide remote support. SAQ D if not qualified for SAQ C	Yes - Off-the-shelf applications must be listed on PCI Security Council's List of Validated Payment Applications; or on Visa's List of Validated Payment Applications (See note above regarding in-house developed or custom built applications.)	Yes. See requirement above for Service Providers
Third Party Service Provider – URL Link only to Provider functioning as a gateway (Pay Now type icon)	No Since data is not processed, transmitted, or stored on merchant's server	SAQ A Must be able to answer questions pertaining to Requirement 12.8	N/A	Yes. See requirement above for Service Providers
Third Party Service Provider – Merchant's website, where payments made, is hosted by a web hosting company	No Since data is not processed, transmitted, or stored on merchant's server	SAQ A Must be able to answer questions pertaining to Requirement 12.8	N/A	Yes. See requirement above for Service Providers

Yahoo Store – URL Link only to Yahoo (Service Provider)	No Since data is not processed, transmitted, or stored on merchant's server	SAQ A Must be able to answer questions pertaining to Requirement 12.8	N/A	Yes. See requirement above for Service Providers
Online Web Application - Using Internet to transmit data to Acquirer	Yes. Since PC is connected to the Internet	SAQ C if data is not stored in electronic format; and the application and Internet connection are on the same device; and application is not connected to any other system; and the application vendor uses secure techniques to provide remote support. SAQ D if not qualified for SAQ C	Yes - Off-the-shelf applications must be listed on PCI Security Council's List of Validated Payment Applications; or on Visa's List of Validated Payment Applications (See note above regarding in-house developed or custom built applications.)	Yes. See requirement above for Service Providers
Online Web Application - Transmitting data to Common Payment Service Gateway	Yes. Since PC is connected to the Internet	SAQ C if data is not stored in electronic format; and the application and Internet connection are on the same device; and application is not connected to any other system; and the application vendor uses secure techniques to provide remote support. SAQ D if not qualified for SAQ C	Yes - Off-the-shelf applications must be listed on PCI Security Council's List of Validated Payment Applications; or on Visa's List of Validated Payment Applications (See note above regarding in-house developed or custom built applications.)	Common Payment Service is validated as a compliant service provider by Trustwave annually
Virtual Card Terminal (VCT) provided by Common Payment Service Gateway or a third-party gateway	Yes. Since agency's PC, functioning as a terminal, is connected to the Internet	SAQ C if data is not stored in electronic format; and the PC is a stand-alone-terminal not connected to any other system. SAQ D if not qualified for SAQ C	N/A	Common Payment Service is validated as a compliant service provider by Trustwave
Third Party Service Provider that only stores backup data - in any type of electronic format (tape or images)	No Unless data is retrieved by merchant and is subsequently stored on the merchant's server network.	SAQ A Must be able to answer questions pertaining to Requirement 12.8	N/A	Yes. See requirement above for Service Providers

Information above is for guidance only and is not intended to be a substitute for requirements specified in the PCI Data Security Standard and related instructions. Consultation with Trustwave Support may be appropriate if there are questions regarding which requirements apply to your agency.