APPLICABILITY OF PCI DATA SECURITY STANDARD (PCI DSS) TO CARD CAPTURE METHODS

NC Office of the State Controller

General Requirements for Merchants

- All merchants <u>and</u> their service providers are required to be compliant with the <u>PCI Data Security Standard</u>.
- 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 <u>Self-Assessment Questionnaire</u> (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 <u>vulnerability</u> <u>scanning</u> 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 <u>vendor-supplied</u> payment applications, the <u>Payment Application Standard</u> (PADSS) 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 <u>must</u> be provided.)
- Capture applications accepting PIN debit cards must adhere to the PCI <u>Pin Transaction Security</u> (PCI PTS), with the PIN device being on the PCI Council's <u>List of Approved PEDs</u>. (Effective July 1, 2010)
- All participants in the MSA with SunTrust Merchant Services must be enrolled in TrustKeeper in order to facilitate their <u>validation requirements</u> ("SAQ Only," or "SAQ <u>and</u> 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
 <u>List of Compliant Service Providers</u> (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	No.	SAQ B if data is not stored	N/A	N/A	
(stand-alone) -	Since no PCs or network	in electronic format.	IV/A	IV/A	
Using analog dial	servers are involved.	in electronic format.			
up telephone line	servers are involved.	SAQ <u>D</u> if not qualified for			
to transmit data to		SAQ D II not quantied for SAQ B			
		SAQB			
the acquirer	Yes.	CAOC if data is not stored	NT/A	NT/A	
POS Terminal		SAQ <u>C</u> if data is <u>not</u> stored	N/A	N/A	
(stand-alone) -	Since POS terminal is	in electronic format.			
Using internet to	connected to a server				
transmit data to	that is connected to the	SAQ <u>D</u> if not qualified for			
the acquirer	Internet	SAQ C			
POS Software	Yes.	SAQ <u>C</u> if data is <u>not</u> stored	Yes – Off-the-shelf	N/A	
Application -	Since PC the POS	in electronic format; and	applications must be		
Using Internet to	software is housed on is	the POS and Internet	listed on PCI		
transmit data to	connected to the Internet	connection are on the same	Security Council's		
the acquirer		device; and POS is not	List of Validated		
-		connected to any other	Payment		
		system; and the POS	Applications; or on		

		vendor uses secure techniques to provide remote support. SAQ <u>D</u> 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 <u>C</u> if data is <u>not</u> stored in electronic format; and POS is <u>not</u> connected to any other system; and the POS vendor uses secure techniques to provide remote support. SAQ <u>D</u> 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 <u>C</u> if data is <u>not</u> stored in electronic format; and the application and Internet connection are on the <u>same</u> device; and application is <u>not</u> connected to any other system; and the application vendor uses secure techniques to provide remote support. SAQ <u>D</u> 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 <u>A</u> 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 <u>A</u> Must be able to answer questions pertaining to Requirement 12.8	N/A	Yes. See requirement above for Service Providers

Yahoo Store –	No	SAQ <u>A</u>	N/A	Yes. See
URL Link only to	Since data is not	Must be able to answer	IV/A	requirement
Yahoo (Service	processed, transmitted,	questions pertaining to		above for
Provider)	or stored on merchant's	Requirement 12.8		Service
1 Tovidet)	server	Requirement 12.0		Providers
Online Web	Yes.	SAQ C if data is not stored	Yes - Off-the-shelf	Yes. See
Application -	Since PC is connected to	in electronic format; and	applications must be	requirement
Using Internet to	the Internet	the application and Internet	listed on PCI	above for
transmit data to	the internet	connection are on the <u>same</u>	Security Council's	Service
Acquirer		device; and application is	List of Validated	Providers
Acquirei		not connected to any other	Payment	Floviders
		system; and the application	Applications; or on	
		vendor uses secure	Visa's <u>List of</u>	
		techniques to provide	Validated Payment	
			Applications	
		remote support.	Applications	
		SAQ D if not qualified for	(See note above	
		SAQ D II not quantied for SAQ C	regarding in-house	
		SAQC	developed or custom	
			built applications.)	
Online Web	Yes.	SAQ C if data is not stored	Yes - Off-the-shelf	Common
Application -	Since PC is connected to	in electronic format; and	applications must be	Payment
Transmitting data	the Internet	the application and Internet	listed on PCI	Service is
to Common		connection are on the <u>same</u>	Security Council's	validated as a
Payment Service		device; and application is	List of Validated	compliant
Gateway		not connected to any other	Payment	service
v		system; and the application	Applications; or on	provider by
		vendor uses secure	Visa's List of	Trustwave
		techniques to provide	Validated Payment	annually
		remote support.	Applications	,
		• •		
		SAQ <u>D</u> if not qualified for	(See note above	
		SAQ C	regarding in-house	
			developed or custom	
Vi-AI C	Vac	CAOC if data is not start.	built applications.)	Comme
Virtual Card	Yes.	SAQ <u>C</u> if data is <u>not</u> stored	N/A	Common
Terminal (VCT)	Since agency's PC,	in electronic format; and		Payment Sarvice is
provided by	functioning as a terminal, is connected to	the PC is a stand-alone-		Service is
Common Payment	<u> </u>	terminal <u>not</u> connected to		validated as a
Service Gateway	the Internet	any other system.		compliant service
or a third-party		SAOD if not avalified for		
gateway		SAQ <u>D</u> if not qualified for SAQ C		provider by Trustwave
Third Party	No	SAQ A	N/A	Yes. See
Service Provider	Unless data is retrieved	Must be able to answer	11/1	requirement
that only stores	by merchant and is	questions pertaining to		above for
backup data - in	subsequently stored on	Requirement 12.8		Service
any type of	the merchant's server	Requirement 12.8		Providers Providers
electronic format	network.			110110618
(tape or images)	HELWOIK.			
(tape of images)				

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 <u>Trustwave Support</u> may be appropriate if there are questions regarding which requirements apply to your agency.