

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

Card Capture Method	Required Vulnerability Scanning of IP Addresses	Required Annual <u>Self-Assessment Questionnaire</u> (SAQ)	Compliance w/ Payment Application Standard	Service Provider Subject to PCI DSS
<p>All merchants are required to be compliant with the PCI Data Security Standard. For any environment under which un-masked cardholder data is stored electronically, SAQ <u>D</u> applies. For any environment involving web-facing IP addresses, vulnerability scanning is required. For any environment using vendor-supplied payment applications, the Payment Application Standard applies.</p>				
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 <u>B</u> if data is <u>not</u> stored in electronic format. SAQ <u>D</u> 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 <u>C</u> if data is <u>not</u> stored in electronic format. SAQ <u>D</u> 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 <u>C</u> if data is <u>not</u> stored in electronic format; and the POS and Internet connection are on the <u>same</u> device; 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 - Must be listed on Visa's List of Validated Payment Applications 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.	N/A
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 - Must be listed on Visa's List of Validated Payment Applications 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.	N/A
Third Party Service Provider – Card data captured by merchant and then transmitted to Provider	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	Yes - Must be listed on Visa's List of Validated Payment Applications In-house applications developed by merchants or service providers that are not sold to a third party	Yes. Must be on Visa's List of Compliant Service Providers

		remote support. SAQ <u>D</u> if not qualified for SAQ <u>C</u>	are not subject to the PA-DSS, but subject to PCI DSS.	
Third Party Service Provider – URL Link only to Provider (Pay Now type icon)	No Since data is not processed, transmitted, or stored on merchant’s server	SAQ <u>A</u>	N/A	Yes. Service Provider must to validated as compliant by a QSA.
Yahoo Store – URL Link only to Yahoo (Service Provider)	No Since data is not processed, transmitted, or stored on merchant’s server	SAQ <u>A</u>	N/A	Yes. Yahoo must be validated as compliant by a QSA.
Online Web Application - Using Internet to transmit data to Acquirer	Yes. Since PC is connected to the Internet	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 <u>C</u>	Yes - Must be listed on Visa’s List of Validated Payment Applications 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.	Common Payment Service is validated as a compliant service provider by Trustwave annually
Online Web Application - Transmitting data to Common Payment Service Gateway	Yes. Since PC is connected to the Internet	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 <u>C</u>	Yes - Must be listed on Visa’s List of Validated Payment Applications 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.	Common Payment Service is validated as a compliant service provider by Trustwave annually
Virtual Card Terminal (VCT) provided by Common Payment Service Gateway	No Since data is not processed, transmitted, or stored on merchant’s server	SAQ <u>A</u> if for card-not-present transactions (mail order , telephone) SAQ <u>B</u> if for card-present transactions (presented card is keyed)	N/A	Common Payment Service is validated as a compliant service provider by Trustwave

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.