PCI DSS v3.0 SAQ Eligibility

http://www.ambersail.com

Disclaimer: The information in this document is provided "as is" without warranties of any kind, either express or implied, including, without limitation, implied warranties of merchantability or fitness for a particular purpose.

SAQ	Description	Eligibility Criteria
SAQ A	*Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced*	*This SAQ is not applicable to face-to-face channels* • **Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);** • All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers; • Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored; • Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions; • Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and • Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically. *Additionally, for e-commerce channels:* • The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

SAQ	Description	Eligibility Criteria
SAQ A-EP	*Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing*	*This SAQ is only applicable only to e-commerce channels* • **Merchant accepts only e-commerce transactions;** • All processing of cardholder data is outsourced to a PCI DSS validated third-party payment processor; • Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor; • Merchant's e-commerce website is not connected to any other systems within merchant's environment (this can be achieved via network segmentation to isolate the website from all other systems); • If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider); • All elements of payment pages that are delivered to the consumer's browser originate from either the merchant's website or a PCI DSS compliant service provider(s); • Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions; • Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and • Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

SAQ	Description	Eligibility Criteria
SAQ B	*Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals— No Electronic Cardholder Data Storage*	*This SAQ is not applicable to e-commerce channels* • **Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data over either a phone line or the Internet; and/or Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment**; • Merchant does not transmit cardholder data over a network (either an internal network or the Internet); • Merchant does not store cardholder data in electronic format; and • If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.
SAQ B-IP	*Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage*	*This SAQ is not applicable to e-commerce channels* • **Merchant uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to merchant's payment processor to take customers' payment card information;** • The standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs); • The standalone IP-connected POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate POI devices from other systems); • The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor; • The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor; • Merchant retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and • Merchant does not store cardholder data in electronic format.

SAQ	Description	Eligibility Criteria
SAQ C	*Merchants with Payment Application Systems Connected to the Internet— No Electronic Cardholder Data Storage*	*This SAQ is not applicable to e-commerce channels* • **Merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);** • The payment application system/Internet device is not connected to any other system within the merchant environment; • The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only; • Merchant does not store cardholder data in electronic format; and • If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.
SAQ C-VT	*Merchants with Web-Based Virtual Payment Terminals—No Electronic Cardholder Data Storage*	*This SAQ is not applicable to e-commerce channels* • **Merchant's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;** • Merchant's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider; • Merchant accesses the PCI DSS-compliant virtual terminal solution via a computer that is isolated in a single location and is not connected to other locations or systems within the merchant environment; • Merchant's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward); • Merchant's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached); • Merchant does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet); • Merchant does not store cardholder data in electronic format; and • If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.

SAQ	Description	Eligibility Criteria
SAQ P2PE-HW	*Hardware Payment Terminals in a PCI-Listed P2PE Solution Only – No Electronic Cardholder Data Storage*	*SAQ P2PE-HW has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.* • **All payment processing is via the validated P2PE solution approved by the PCI SSC (per above).** • The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution. • Merchant does not otherwise receive or transmit cardholder data electronically. • Merchant verifies there is no legacy storage of electronic cardholder data in the environment. • If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically, and Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.
SAQ D Merchant	*All other SAQ-Eligible Merchants*	*SAQ D for Merchants applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type*
SAQ D Service Providers	*SAQ-Eligible Service Providers*	*SAQ D for Service Providers applies to all service providers defined by a payment brand as being SAQ-eligible.*