

Selecting the SAQ and Attestation that Best Apply to Your Organization

According to payment brand rules, all merchants and service providers are required to comply with the PCI DSS in its entirety. There are five SAQ categories, shown briefly in the table below and described in more detail in the following paragraphs. Use the table to gauge which SAQ applies to your organization, then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants.</i>
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.

SAQ A – Card-not-present Merchants, All Cardholder Data Functions Outsourced

SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their systems or premises.

For a graphical guide to choosing your SAQ type, please see “Which SAQ Best Applies to My Environment?” on page 17.

SAQ A merchants do not store cardholder data in electronic format, do not process or transmit any cardholder data on their systems or premises, and validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that the third party(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

This option would never apply to merchants with a face-to-face POS environment.

SAQ B – Merchants with Only Imprint Machines or Only Standalone, Dial-Out Terminals. No Electronic Cardholder Data Storage.

SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals.

SAQ B merchants only process cardholder data via imprint machines or via standalone, dial-out terminals, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants. Such merchants validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

- Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- Your company does not transmit cardholder data over a network (either an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store cardholder data in electronic format.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 17.

SAQ C-VT – Merchants with Web-Based Virtual Terminals, No Electronic Cardholder Data Storage

SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual terminals on personal computers connected to the Internet.

A virtual terminal is web-browser based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

These merchants process cardholder data only via a virtual terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution.

SAQ C-VT merchants process cardholder data via virtual terminals on personal computers connected to the Internet, do not store cardholder data on any computer system, and may be brick-and-mortar

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 17.

(card-present) or mail/telephone-order (card-not-present) merchants. Such merchants validate compliance by completing SAQ C-VT and the associated Attestation of Compliance, confirming that:

- Your company's only payment processing is done via a virtual terminal accessed by an Internet-connected web browser;
- Your company's virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company 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 your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- Your company'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);
- Your company'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);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts; **and**
- Your company does not store cardholder data in electronic format.

This option would never apply to e-commerce merchants.

SAQ C – Merchants with Payment Application Systems Connected to the Internet, No Electronic Cardholder Data Storage

SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.) either because:

1. *The payment application system is on a personal computer that is connected to the Internet (for example, for e-mail or web browsing), or*
2. *The payment application system is connected to the Internet to transmit cardholder data.*

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 17.

SAQ C merchants process cardholder data via POS machines or other payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. SAQ C merchants validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company 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 systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- Your company store is not connected to other store locations, and any LAN is for a single store only;

- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; **and**
- Your company's payment application software vendor uses secure techniques to provide remote support to your payment application system.

SAQ D – All Other Merchants and All Service Providers Defined by a Payment Brand as Eligible to Complete an SAQ

SAQ D has been developed for all service providers defined by a payment brand as eligible to complete an SAQ, as well as SAQ-eligible merchants who do not meet the descriptions of SAQ types A through C, above.

SAQ D service providers and merchants validate compliance by completing SAQ D and the associated Attestation of Compliance.

While many of the organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. See the guidance below for information about the exclusion of wireless technology and certain other, specific requirements.

Guidance for Non-Applicability of Certain, Specific Requirements

Exclusion: If you are required to answer SAQ C or D to validate your PCI DSS compliance, the following exceptions may be considered. See “Non-Applicability” below for the appropriate SAQ response.

- Requirements 1.2.3, 2.1.1 and 4.1.1 (SAQs C and D): These questions specific to wireless only need to be answered if wireless is present anywhere in your network. Note that Requirement 11.1 (use of a process to identify unauthorized wireless access points) must still be answered even if wireless is not in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- Requirements 6.3 and 6.5 (SAQ D): These questions are specific to custom applications and code, and only need to be answered if your organization develops its own custom applications.
- Requirements 9.1 through 9.4 (SAQ D): These questions only need to be answered for facilities with “sensitive areas” as defined here. “Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data.

Non-Applicability: For all SAQs, these and any other requirements deemed not applicable to your environment must be indicated with “N/A” in the “Special” column of the SAQ. Accordingly, complete the “Explanation of Non-Applicability” worksheet in the SAQ Appendix for each “N/A” entry.

Instructions for Completing the SAQ

1. Use the guidelines herein to determine which SAQ is appropriate for your company.
2. Use *Navigating PCI DSS: Understanding the Intent of the Requirements* to understand how and why the requirements are relevant to your organization.
3. Assess your environment for compliance with the PCI DSS.
4. Use the appropriate Self Assessment Questionnaire as a tool to validate compliance with the PCI DSS.
5. Follow the instructions in the appropriate Self-Assessment Questionnaire at “PCI DSS Compliance – Completion Steps,” and provide all required documentation to your acquirer or payment brand as appropriate.

Which SAQ Best Applies to My Environment?

