

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 Data Security Standard in its entirety. There are five SAQ Validation 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 Validation Type	Description	SAQ
1	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>	A
2	Imprint-only merchants with no cardholder data storage	B
3	Stand-alone dial-up terminal merchants, no cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

SAQ Validation Type 1 / SAQ A: *Card-not-present, 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 premises.

Merchants in Validation Type 1 do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises, and must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on a third party to handle these functions;
- Your company has confirmed that the third party 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.

For a graphical guide to choosing your validation type, please see “SAQ Instructions and Guidelines—What is my Validation Type” on page 12.

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

SAQ Validation Type 2 / SAQ B: *Imprint Merchant Only, 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 stand-alone dial-up terminals.

Merchants in Validation Type 2 only process cardholder data via imprint machines, and must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

- Your company uses only an imprint machine to take your customers' payment card information;
- Your company does not transmit cardholder data over either a phone line or the Internet;
- Your company retains only paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

For a graphical guide to choosing your validation type, please see "SAQ Instructions and Guidelines—What is my Validation Type" on page 12.

SAQ Validation Type 3 / SAQ B: *Standalone, Dial-out Terminal Merchant, 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 stand-alone dial-up terminals.

Merchants in Validation Type 3 process cardholder data via stand-alone, dial-out terminals, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants. Merchants in Validation Type 3 must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

- Your company uses only standalone, dial-out terminals (connected via a phone line to your processor);
- 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 retains only paper reports or paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

SAQ Validation Type 4 / SAQ C: *Merchants with Payment Application Systems Connected to the Internet*

SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale or shopping cart systems) are connected to the Internet (via high-speed connection, 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.

Merchants in Validation Type 4 process cardholder data via 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. Merchants in

Validation Type 4 must 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;
- The payment application system/Internet device is not connected to any other systems within your environment;
- 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.

For a graphical guide to choosing your validation type, please see "SAQ Instructions and Guidelines—What is my Validation Type" on page 12.

SAQ Validation Type 5 / 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 to address requirements applicable to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under Validation Types 1-4 above.

Service providers and merchants in Validation Type 5 must 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 wireless technology. See the guidance below for information about the exclusion of wireless technology and certain other, specific requirements.

Guidance for Non-Applicability and Exclusion 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 (SAQ D), 2.1.1 (SAQs C and D), and 4.1.1 (SAQ 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 wireless analyzer) must still be answered even if wireless is not in your network, since the analyzer detects any rogue or unauthorized devices that may have been added without your knowledge.
- Requirements 6.3-6.5 (SAQ D): These questions specific to custom applications and code only need to be answered if your organization writes its own custom web applications.
- Requirements 9.1-9.4 (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.

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 Appendix for each "N/A" entry.

SAQ Instructions and Guidelines—What is My Validation Type?

