PCI

Compliance Tool

for Merchants and Service Members

PCI SAQ A

TABLE OF CONTENTS

Understanding PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is the global data security standard that businesses of all sizes must adhere to when accepting payment cards. It presents user-friendly steps that reflect best security practices.

The goal of this guide is to help you complete your Self-Assessment Questionnaire (SAQ) A and validate your compliance with PCI DSS.

Qualifying as a SAQ A Merchant

SAQ A addresses these requirements:

- Your company accepts only card-not-present (E-Commerce or mail/telephone-order) transactions.
- All payment acceptance and processing are completely outsourced to PCI DSS-validated third parties.
- Your company has no direct control of the way that cardholder data is captured, processed, transmitted, or stored.
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises. Instead, it relies completely on a third party to handle these.
- Your company has confirmed that all third parties handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS-compliant.
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

For E-Commerce channels:

- All payment pages delivered to the consumer's browser originate directly from third-party PCI DSS-validated service providers.

Understanding Types of SAQ Eligibility

SAQ A does not apply to merchants with a face-to-face Point-of-Sale (POS) environment. Following are the different SAQ types and their descriptions.

SAQ Type	Description
A	Card-not-present (E-Commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This does not apply to face-to-face merchants.
A-EP	E-Commerce merchants who outsource their transactions to PCI DSS-validated third parties and do not store electronic cardholder data.
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage.
B-IP	Card-present or mail/telephone-order (card-not-present) merchants who process through point-of-interaction devices with IP connection. There is no electronic cardholder data storage.
C-VT	Merchants using only Web-based virtual terminals. There are no card readers or electronic cardholder data storage.
C	Merchants with payment application systems connected to the Internet. There is no electronic cardholder data storage.
D	Merchants with payment application systems connected to the Internet. There is no electronic cardholder data storage.
P2PE	Merchants processing with point-to-point hardware terminals that are PCI-listed/validated. There is no storing, processing, or transmitting outside of the P2PE terminal.

There are 12 requirements defined in the PCI DSS. SAQ A contains a few of the questions from two of those requirements.

- **Requirement 9 – Restrict physical access to cardholder data.**
- **Requirement 12 – Maintain a policy that addresses information security.**

The answer guide below will help you complete the questions for each of these requirements.

Understanding Common SAQ Questions

When you take your SAQ A, you must answer questions from Requirements 9 and 12. Here are some common SAQ questions you must answer to stay compliant.

Requirement 9

Question	**Answer**
Are all media physically secured (including, but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? For Requirement 9, “media” refers to all paper and electronic media containing cardholder data.	Yes
Is strict control maintained over the internal or external distribution of any kind of media?	Yes
Is media classified so that the sensitivity of the data can be determined?	Yes
Is media sent by secured courier or other delivery method that can be accurately tracked?	Yes
Is management approval obtained before moving the media, especially when media is distributed to individuals?	Yes
Is strict control maintained over the storage and accessibility of media?	Yes

Is all media destroyed when it is no longer needed for business or legal reasons?	Yes
Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	Yes
Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	Yes

Requirement 9 Answers:

These questions are related to the physical handling and access of cardholder data. Answer “Yes” to them if you:

- Keep the data physically secure at all times.
- Monitor all movement.
- Destroy it when no longer needed for business or legal reasons, so that it can never be reconstructed.

Requirement 12

Question	**Answer**
Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data?	Yes
Is a list of service providers maintained?	Yes

Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?	Yes
Is there an established process for engaging service providers, including proper due diligence before engagement?	Yes
Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	Yes
Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	Yes

Requirement 12 Answers:

All of these questions relate to having policies and procedures in place to distribute to all employees. Best practices require that you manage and monitor service providers. You should also have a policy in place that covers information security responsibilities.

If you do not currently have policies and procedures in place, use the template below to develop a policy for your organization, and distribute it to all employees. Best practices require you to customize and implement the policy so you can answer "Yes." Formally review the policy with all employees annually, and have each employee sign an acknowledgement of receipt that you can file.

We hope that this guide has helped you complete your SAQ. For assistance, contact your ISO or payment processor.