securitymetrics®

PCI SAQ Overview

Never have a false sense of security.™

A

31 Questions, Vuln. Scan

Ecommerce website (third party)

- Fully outsourced card acceptance and processing
- Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor
- Merchant can't impact the security of the payment transaction

A-EP

151 Questions, Vuln. Scan

Ecommerce website (direct post)

- Merchant website accepts payment using direct post or transparent redirect service

B

27 Questions, No Scan

Processes cards via:

- Analog phone, fax, or stand-alone terminal
- Cellular phone (voice) or stand-alone terminal
- Knuckle buster/imprint machine

B-IP

48 Questions, Vuln. Scan

Processes cards via:

- Internet-based stand-alone terminal isolated from other devices on the network
- Cellular phone (voice) or stand-alone terminal
- Knuckle buster/imprint machine

C

131 Questions, Vuln. Scan

Payment application systems connected to the Internet:

- Virtual terminal (Not C-VT eligible)
- IP terminal (Not B-IP eligible)
- Mobile device (smartphone/tablet) with a card processing application or swipe device
- View or handle cardholder data via the Internet
- POS with tokenization

C-VT

54 Questions, No Scan

Processes cards:

- One at a time via keyboard into a virtual terminal
- On an isolated network at one location
- No swipe device
- Knuckle buster/imprint machine

P2PE

21 Questions, No Scan

Point-to-point encryption

- Validated PCI P2PE hardware payment terminal solution only
- Merchant specifies they qualify for the P2PE questionnaire

SPOC

22 Questions, No Scan

Processes cards:

- Validated SPoC solution only
- Merchant specifiies they qualify for the SPoC questionnaire

D-Merchant

251* Questions, Vuln. Scan

Ecommerce website

- Merchant website accepts payment and does not use a direct post or transparent redirect service

Electronic storage of card data

- POS system not utilizing tokenization or P2PE
- Merchant stores card data electronically (e.g., email, e-fax, recorded calls, etc.)

D-Service Provider

267** Questions, Vuln. Scan

Service Provider

- Handles card data on behalf of another business
- Provides managed firewalls in another entity's cardholder data environment
- Hosts a business's ecommerce environment/website or controls the flow of ecommerce data.

**Additional controls in Appendix A2 of the PCI standard.*
***Additional controls in Appendix A1 and A2 of the PCI standard.*

DETERMINE YOUR SAQ TYPE

How you process credit cards and handle cardholder data determines which of the 10 Self-Assessment Questionnaire (SAQ) types your business needs to fill out. Here are the different SAQ type requirements:

SAQ A

- Your company only accepts card-not-present (ecommerce or mail/telephone-order) transactions.
- All processing of cardholder data is entirely outsourced to a PCI DSS validated third-party service provider(s).
- Your company does not electronically 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 providers are PCI DSS compliant for the services they are providing.
- Any cardholder data your company retains is on paper (such as printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the ecommerce payment page(s) delivered to the customer's browser originate from PCI DSS compliant providers or processors.
- Your company has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

In summary, if your company has completely outsourced the collection and processing of cardholder data to PCI DSS-compliant third-party providers and your employees never have access to full credit card numbers, there is a strong likelihood that the SAQ A is the appropriate SAQ for your environment.

SAQ A UPDATED CRITERIA

There are three main ways merchants collect card data that may qualify them for SAQ A:

- All of the shopping cart and payment web site is totally outsourced to a PCI DSS compliant 3rd party (all content and payment pages), this may also reduce even the number of SAQ A requirements a merchant is required to validate.
- Your website uses a full redirect method (like a pay now button) that sends the customer to a separate URL for checkout that is hosted by a PCI DSS compliant service provider.
- Your website contains an iframe element that contains a payment page hosted by a PCI DSS compliant service provider.

A new change for SAQ A was made in early 2025 that removed the PCI DSS script security requirements 6.4.3 and 11.6.1 from the list to be validated by an entity.

These requirements were replaced by new eligibility criteria that must be met in order to qualify an entity to use SAQ A. Careful reading of these eligibility statements show that an entity is not totally off the hook when it comes to protection from malicious card skimming scripts being added to pages that contain e-commerce elementsents (e.g., iframe used to display third party payment page).

The statement says “the merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).” This means that the merchant has to be using active security controls to protect their site (this really refers to payment pages, as was the scope for 6.4.3 and 11.6.1 originally) from the execution of malicious scripts that target e-commerce elements. You can also refer to **FAQ 1588** written by the PCI Security Standards council to help with the interpretation of the eligibility criteria added.

Additionally the criteria implies a need for evidence to support the assertion that the site is not susceptible.

This evidence would need to come from one of the following sources:

- A system the merchant creates themselves (very difficult to do correctly)
- The merchant could contract with a service built to monitor sites for the presence of data skimming scripts
- Get a written statement (or entry on a responsibility matrix) from a TPSP stating that they will provide services or controls that meet the eligibility criteria of SAQ A for the merchant
- Full compliance to PCI DSS requirements 6.4.3 and 11.6.1

If you can not meet the eligibility statement for SAQ A, then it may be more appropriate to use SAQ A-EP.

SAQ A-EP

- Your company only accepts ecommerce transactions.
- All processing of cardholder data–with the exception of the payment page–is entirely outsourced to a PCI DSS validated third-party payment processor.
- Your ecommerce 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.
- If the 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).
- Each element of the payment page(s) delivered to a consumer's browser originates from your website or a PCI DSS compliant service provider(s).
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on third parties to handle all of these functions.
- Your company has confirmed that all third parties handling storage, processing, and transmission of cardholder data are PCI DSS compliant.
- Any cardholder data your company retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.

Like most SAQ A merchants, SAQ A-EP merchants have an ecommerce payment environment where the collection and processing of cardholder data have been outsourced to PCI DSS-compliant service providers. Unlike the SAQ A, SAQ A-EP websites control the flow of cardholder data to the service provider (typically using javascript or direct post methods).

If you have an ecommerce environment and you are not using a third-party iFrame or fully redirecting users to the service provider's website for payment collection but your website never receives cardholder data directly, the SAQ A-EP is likely the correct choice for your compliance documentation.

SAQ B

- Your company only uses 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.
- Standalone, dial-out terminals are not connected to any other systems within your environment.
- 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).
- Any cardholder data your company retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Most SAQ B merchants receive cardholder data in person and via mail-order/telephone-order transactions and process these payments using bank-provided payment terminals that are connected to dial-up/analog phone lines. Cardholder data should never be received electronically (via email) or stored electronically. Be sure your terminals are connected to analog lines and not connected to IP networks.

SAQ B-IP

- Your business only uses standalone, PTS-approved Point of Interaction (POI) devices connected via IP to your payment processor to take your customers' payment card data.
- Standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs).
- Standalone IP-connected POI devices are not connected to any other systems within your environment.
- The only transmission of cardholder data is from PTS-approved POI devices to the payment processor.
- The POI device doesn't rely on any other device (e.g., computer, mobile phone, tablet) to connect to the payment processor.
- The business has only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically.
- Your company does not store cardholder data electronically.

Most SAQ B-IP merchants receive cardholder data in person and via mail-order/telephone-order transactions and process these payments using bank-provided terminals.

SAQ B-IP terminals are, however, connected to an IP network and transmit their data over the network instead of an analog connection. This allows for much faster processing times, but security controls must be in place to properly segment and protect payment data being transmitted over the network.

SAQ C

- Your business has a payment application system and an Internet connection on the same device and/or same local area network (LAN).
- The payment application system isn't connected to any other systems within your environment.
- The POS environment isn't connected to other locations, and any LAN is for a single location only.
- Any cardholder data your business retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Typical SAQ C merchants receive cardholder data in person and via mail-order/telephone-order transactions that are processed using a Point-of-Sale system that is configured to not store the full PAN (credit card number). Typical POS solutions will have multiple POS workstations/registers connected to a back-end server (the server may be hosted by a vendor/third-party). The SAQ C is designed for a simple, single-location POS deployment.

Merchants with multiple locations that are connected to the corporate office should be using the SAQ D.

SAQ C-VT

- Your company only processes payments through a virtual payment terminal accessed by an Internet-connected web browser.
- Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider.
- Your company accesses the PCI DSS-compliant virtual payment terminal solution through a computer that is isolated in a single location and is not connected to other locations or systems within your environment.
- Your company's computer does not have software installed that causes cardholder data to be stored.
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data.
- Your company does not otherwise receive or transmit cardholder data electronically through any channels.
- Any cardholder data your company retains is on paper, and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Typically, SAQ C-VT merchants receive cardholder data in person and via mail-order/telephone-order transactions and enter the data into a PCI-compliant web-based virtual terminal using a workstation dedicated to processing payments. Workstations used to enter payment data into the third-party virtual terminal must be on an isolated network segment. Network security controls must be configured to allow only traffic required to perform this business function. All other inbound and outbound traffic to the network segment must be blocked.

SAQ P2PE

- All payment processing is through a validated PCI P2PE solution approved and listed by the PCI SSC.
- 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.
- You do not otherwise receive or transmit cardholder data electronically.
- There's no legacy storage of electronic cardholder data in the environment.
- If your business stores cardholder data, this data is only in paper reports or copies of paper receipts and isn't received electronically.
- Your business has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

In order to reduce risk in a merchant payment environment and to minimize the efforts to maintain PCI DSS compliance, the PCI SSC has developed a standard for point-to-point encryption solutions. P2PE payment solutions will strongly encrypt cardholder data at the point of entry (POI device) and send the encrypted data to the P2PE solution provider for decryption and processing.

Typical SAQ P2PE merchants receive cardholder data in person and via mail-order/telephone-order transactions and process the payments using validated P2PE terminals (a list of validated P2PE solutions can be found on the PCI Council's website).

SAQ D FOR MERCHANTS

SAQ D applies to merchants who don't meet the criteria for any other SAQ type. This SAQ type handles merchants who store card information electronically and do not use a P2PE certified POS system. Examples of SAQ D merchant types include:

- Ecommerce merchants who accept cardholder data on their website.
- Merchants with electronic storage of cardholder data.
- Merchants that don't store cardholder data electronically, but that do not meet the criteria of another SAQ type.
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

SAQ D FOR SERVICE PROVIDERS

A service provider is a business entity that isn't a payment brand, but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another organization.

Service providers can also provide services that control or could impact the security of cardholder data processed under another company's merchant account.

Examples of service providers who qualify for SAQ D include:

- A service provider that handles card data on behalf of another business.
- A service provider that provides managed firewalls in another entity's cardholder data environment.
- A service provider that hosts a business's ecommerce environment/website or controls the flow of ecommerce data.

SAQ SPOC

- All payment processing is only via a card-present payment channel.
- All cardholder data entry is via a Secure Card Reader PIN (SCRP) that is part of a validated SPoC solution approved and listed by PCI SSC (Payment Card Industry Security Standards Council).
- The only systems in the merchant's SPoC environment that store, process, or transmit account data are those used as part of the validated SPoC solution approved and listed by PCI SSC.
- The merchant does not otherwise receive, transmit, or store account data electronically.
- This payment channel is not connected to any other systems/networks within the merchant environment.
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
- The merchant has implemented all controls in the SPoC user guide provided by the SPoC Solution Provider.

Based on these eligibility criteria, we know that ecommerce payment channels will not qualify for SAQ SPoC assessments. All payments must be card-present where the credit card details are captured using a device that is part of a validated SPoC solution.

Due to the limited number of validated SPoC solutions at this time, very few merchants will qualify to use this self-assessment questionnaire.

COMBINING MULTIPLE SAQS

Some merchants will have multiple payment flows that together may not fit any SAQ type besides the SAQ D. For instance, a merchant may have an outsourced ecommerce payment channel that would fit the SAQ A but may also accept card-present transactions using an analog-connected bank terminal (SAQ B).

A merchant with multiple payment channels will likely be required to complete the SAQ D as they would not be able to affirmatively answer the qualifying criteria questions when looking at their multiple payment channels together.

Some merchant banks will allow a merchant to assess each payment channel separately with the SAQ that matches each payment channel. So, in the case of an SAQ A + SAQ B combo environment, the merchant may be able to complete an SAQ A to cover their ecommerce channel and an SAQ B to cover the card-present payment channel and provide their bank with both SAQs.

If your merchant environment consists of two or more simple payment channels, it may be worth your time to have a conversation with your merchant bank to see if you would be able to assess each payment channel separately.

ABOUT SECURITYMETRICS

We secure peace of mind for organizations that handle sensitive data. We hold our tools, training, and support to a higher, more thorough standard of performance and service.

We are a PCI certified Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Certified Forensic Investigator (PFI), and Managed Security provider with over 20 years of data security experience. From local shops to some of the world's largest brands, we help all businesses achieve data security through managed services and compliance mandates (PCI, HIPAA, GDPR, HITRUST). We have tested over 1 million systems for data security and compliance. We are privately held and are headquartered in Orem, Utah, where we maintain a Security Operations Center (SOC) and 24/7 multilingual technical support.

www.securitymetrics.com/pci