

How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?

PCI SSC FAQ | Article 1588 | February 2025

This FAQ is only intended to clarify the specific SAQ A eligibility criteria called out below. The contents of this FAQ should not be interpreted to impact or contradict any other eligibility criteria in SAQ A or in any other SAQ.

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ) A r1 includes the following eligibility criteria for e-commerce channels:

The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s). *

* Refer to the latest version of PCI DSS SAQ A for the complete list of eligibility criteria.

The above SAQ A eligibility criteria only applies to e-commerce merchants with a webpage that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frame(s) (iframes)).

The above SAQ A eligibility criteria does not apply to e-commerce merchants with a webpage that redirects customers from the merchant's webpage to a TPSP/payment processor (for example, including but not limited to, with an HTTP 30x redirect, a meta redirect tag, or a JavaScript redirect) or e-commerce merchants that fully outsource payment functions to a TPSP/payment processor (for example, by providing customers with an email with a link to a TPSP's website to pay).

The merchant can confirm that the merchant's webpage is not susceptible to script attacks by either:

- Using techniques such as, but not limited to, those detailed in PCI DSS Requirements 6.4.3 and 11.6.1 to protect the merchant's webpage from scripts targeting account data. These techniques may be deployed by the merchant or a third party.

Or

- Obtaining confirmation from the merchant's PCI DSS compliant TPSP/payment processor providing the embedded payment page/form(s) that, when implemented according to the TPSP's/payment processor's instructions, the TPSP's/payment processor's solution includes techniques that protect the merchant's payment page from script attacks.

Merchants are encouraged to work with the merchant's TPSP to obtain guidance about how to implement the TPSP's solution securely.

A provider of third-party scripts is not considered a third-party service provider (TPSP) for purposes of SAQ A, if the provider's only service is providing scripts not related to payment processing and where those scripts cannot impact the security of cardholder data and/or sensitive authentication data.

Merchants should continue to consult with their compliance-accepting entity, the entity to which the SAQ will be submitted (typically, an acquirer (merchant bank) or the payment brands), to determine if the merchant is required to submit an SAQ, and if so, which SAQ is appropriate for the merchant's environment.

Contact information for the payment brands can be found in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

See also:

FAQ 1133: Why are there multiple PCI DSS Self-Assessment Questionnaires (SAQs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/why-are-there-multiple-pci-dss-self-assessment-questionnaires-saqs/)

Source: <https://www.pcisecuritystandards.org/faqs/1588/>