

How are third-party service providers (TPSPs) expected to demonstrate PCI DSS compliance for TPSP services that meet customers' PCI DSS requirements or may impact the security of a customer's cardholder data and/or sensitive authentication data?

PCI SSC FAQ | Article 1065 | November 2024

A TPSP is expected to provide evidence of compliance with applicable PCI DSS requirements.

If the TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer, and that the relevant PCI DSS requirements were examined and determined to be in place. If the provider has an PCI DSS Attestation of Compliance (AOC), it is expected that the TPSP provides the AOC to customers upon request.

If the TPSP does not undergo its own PCI DSS assessment and therefore does not have an AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that the customer (or its assessor) is able to confirm that the TPSP is meeting those PCI DSS requirements.

Note: A TPSP that only provides evidence that it meets a limited set of SAQ requirements applicable to a merchant (for example, SAQ A or an SAQ A Attestation of Compliance (AOC)) has not provided sufficient evidence of PCI DSS compliance for its merchant customers. For more information, refer to the PCI DSS section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers.

Refer to the following FAQs:

FAQ 1221: To which types of service providers does PCI DSS Appendix A1 apply? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/To-which-types-of-service-providers-does-PCI-DSS-Appendix-A1-apply/)

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/)

FAQ 1576: What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-evidence-is-a-TPSP-expected-to-provide-to-customers-to-demonstrate-PCI-DSS-compliance/)