

What is the scope of a PCI DSS assessment for service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data?

PCI SSC FAQ | Article 1580 | June 2024

The scope of a PCI DSS assessment for service providers that can impact the security of payment account data (which consists of cardholder data and/or sensitive authentication data), but which do not directly store, process, or transmit payment account data includes all people, processes, and technology involved in providing the service provider's services.

While the applicable PCI DSS requirements for these service provider assessments will depend on the services provided and the access the service provider may have into a CDE or to payment account data, here are some considerations when scoping a service provider's PCI DSS assessment:

- If the service provider has access to a customer's CDE, to a customer's payment account data, and/or to system components that may allow access to a customer's CDE, the applicable PCI DSS requirements are those that verify network and security controls effectively limit the service provider's access to only that which is necessary.
- If a service provider's services directly or indirectly meet a PCI DSS requirement(s) on behalf of another entity, the applicable PCI DSS requirements are those specific to the service being met by the service provider.
- If a service provider's service that directly or indirectly facilitates storage, processing, and/or transmission of another entity's payment account data, the applicable PCI DSS requirements are those related to the security of the service and systems.

The service provider and its assessor should work together to confirm the applicable PCI DSS requirements, based on an analysis of the service provider's services and the access the service provider has, or may have, to another entity's payment account data, and how and whether that service provider may be able to impact the security of another entity's payment account data.

Where a service provider is completing SAQ D for Service Providers and is not using an external assessor, the applicable PCI DSS requirements should be confirmed by internal staff responsible for compliance.

All PCI DSS requirements determined to be not applicable must be thoroughly justified and documented, either 1) in the ROC along with each requirement for which "Not Applicable" is selected or 2) in SAQ D for Service providers, Appendix C: Explanation of Requirements Noted as Not Applicable.

For any entity seeking to outsource payment or security-related services to a service provider where that service could impact the security of the entity's payment account data, it is important to establish agreements about how PCI DSS compliance

information will be shared between both parties and what type of information the service provider will share to verify that all applicable PCI DSS requirements are being met.

For guidance on nested service providers (where one service provider uses other service providers), refer to the Third-Party Security Assurance Information Supplement.

Also refer to the following FAQs:

- FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-does-encrypted-cardholder-data-impact-pci-dss-scope-for-third-party-service-providers/)
- FAQ 1579: Does PCI DSS assessment apply to service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/does-pci-dss-apply-to-service-providers-that-can-impact-the-security-of-payment-account-data-if-the-service-provider-does-not-directly-store-process-or-transmit-payment-account-data/)

Source: <https://www.pcisecuritystandards.org/faqs/1580/>