

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?

PCI SSC FAQ | Article 1579 | June 2024

Yes. PCI DSS is intended for all entities that store, process, or transmit cardholder data and/or sensitive authentication data or could impact the security of payment account data (which consists of cardholder data and/or sensitive authentication data). This includes all entities involved in payment account processing—including service providers that can impact the security of a cardholder data environment (CDE). Examples of ways a service provider may impact the security of a CDE include, but are not limited to, where the service provider:

- Has direct or indirect access to a customer's CDE, payment account data, and/or system components that may allow access to a customer's CDE.
- Provides a service that directly or indirectly meets a PCI DSS requirement(s) on behalf of another entity (for example, provision of network security controls or anti-malware services).
- Provides a service that directly or indirectly facilitates storage, processing, and/or transmission of another entity's payment account data (for example, passing a URL redirect from one entity to another).

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 1580: 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? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/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/)

Source: <https://www.pcisecuritystandards.org/faqs/1579/>