

How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)?

PCI SSC FAQ | Article 1312 | February 2024

When an entity (the TPSP customer) uses one or more TPSPs for functions within or related to the customer's cardholder data environment, it will impact the customer's PCI DSS compliance, specifically with PCI DSS Requirement 12.8 and with any PCI DSS requirements the TPSP is meeting on the customer's behalf.

In all scenarios where a TPSP is used, the customer must manage and oversee all their TPSP relationships and monitor the PCI DSS compliance status of their TPSPs in accordance with Requirement 12.8. This includes performing due diligence, having appropriate agreements in place, identifying which requirements apply to the customer and which apply to the TPSP, and monitoring the compliance status of TPSPs at least annually. Requirement 12.8 does not specify that the customer's TPSPs must be PCI DSS compliant, only that the customer monitors their compliance status as specified in the requirement. Therefore, TPSPs do not need to be validated as PCI DSS compliant for the customer to meet Requirement 12.8.

However, if a TPSP provides a service that meets a PCI DSS requirement(s) on behalf of the customer, then those requirements are in scope for the customer's assessment and the TPSP's compliance of that service will impact the customer's compliance. For example, if a customer engages a TPSP to manage their network security controls, and the TPSP does not provide evidence that it meets the applicable PCI DSS requirements in PCI DSS Requirement 1, then those requirements are not in place for the customer's assessment. As another example, TPSPs that store cardholder data on behalf of customers need to meet the applicable requirements related to access controls, physical security etc., for their customers to consider those requirements in place for their assessments.

Whether a TPSP is required to undergo a PCI DSS assessment is determined by organizations that manage compliance programs (for example, an acquirer, payment brand, or another entity). Entities should contact the organization that manages their compliance program directly to understand the requirements for TPSPs. Contact details 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/)

Refer to 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/)