

# **Does PCI DSS apply to merchants who outsource all payment processing operations and never store, process or transmit cardholder data?**

PCI SSC FAQ | Article 1092 | June 2025

---

Yes. PCI DSS is intended for any entity that stores, processes, or transmits cardholder data — regardless of whether these activities are conducted directly or by a third-party service provider.

When a merchant outsources its payment processing to a third party and does not store, process, or transmit cardholder data, many PCI DSS requirements may not apply directly to the merchant's environment. However, this does not remove the merchant's responsibility to ensure account data is properly protected by the third party.

Merchants remain responsible for:

- Ensuring the provider is PCI DSS compliant for the services offered,
- Maintaining written agreements with the provider that include acknowledgment of their responsibilities (Requirement 12.8.2),
- Monitoring the provider's compliance status at least annually (Requirement 12.8.4),
- Clearly defining and understanding any shared responsibilities.

Merchants are still required to validate PCI DSS compliance, typically through a Self-Assessment Questionnaire (such as SAQ A). Merchants should confirm their compliance obligations with the organization(s) that manage their compliance program—such as their acquirer or payment brand—also referred to as compliance-accepting entities.

Source: <https://www.pcisecuritystandards.org/faqs/1092/>