

THE VENDOR SAYS THEY ARE PCI COMPLIANT. ASK THESE SEVEN QUESTIONS.

The sentence may be true and still be incomplete for the service, feature, location, responsibility, and period your business relies upon.

PRACTITIONER POSITION

A merchant should not attempt to re-assess every provider, but it should perform enough due diligence to understand what service is covered, by what current evidence, for which activities and locations, with which exclusions and customer responsibilities, and how changes are communicated. Official PCI SSC validation forms matter; a marketing certificate or trust-page badge is not a substitute. The resulting record supports reliance on a provider without turning provider status into the merchant's own compliance conclusion.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A member's ecommerce vendor sends a one-page PCI certificate. The document does not identify the exact service, assessed locations, covered requirements, customer responsibilities, report period, or current status. Sales says this is what every customer receives. The member files it and marks the provider question complete.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- A certificate or badge substitutes for official validation evidence.
- The exact consumed service and feature are not named.
- Customer and shared responsibilities are unavailable or unassigned.
- No owner monitors evidence expiry, service changes, incidents, or exceptions.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Ask seven questions: What exact service do we use? What official current evidence supports it? Is that service in the assessed scope? Which locations and activities are covered? What is excluded or limited? What remains customer or shared responsibility? What change or incident notification will we receive?

Preserve the provider's AOC or other appropriate evidence, service and scope description, responsibility information, dates, limitations, correspondence, and the merchant's own decision record.

Do not convert missing or contradictory documentation into either automatic rejection or blind acceptance. Open a bounded question, identify the affected merchant claim, request correction, and escalate through accountable channels.

Review provider evidence and responsibility at the required cadence supplied by the applicable program and whenever the service, feature, configuration, incident state, or evidence changes.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Does the evidence name the exact service the merchant consumes?

02 Is the evidence an official current validation form rather than a certificate alone?

03 Which merchant duties remain and who owns them?

04 What event reopens the provider reliance decision?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect the service agreement, current official evidence, covered-service description, responsibility information, and known limitations.

02 / MAP

Join the consumed service to provider, customer, and shared activities; evidence; owner; period; and change triggers.

03 / EXPLAIN

Write the narrow reliance claim and any unresolved contradiction without turning it into a universal scope decision.

04 / REDUCE

Remove unsupported assumptions, resolve evidence gaps, assign customer duties, and retire unused services or features.

05 / PROVE

Retain current evidence, correspondence, responsibility decisions, completed customer duties, monitoring, and reopening history.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A PROVIDER'S COMPLIANCE STATEMENT IS AN INPUT TO DUE DILIGENCE-NOT THE CUSTOMER'S COMPLETED CONCLUSION.

Take the Provider Question Card to the next vendor renewal, onboarding, or trust-center review.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0002 / How is an entity's PCI DSS compliance impacted by using TPSPs? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0023 / FAQ 1065: What is a TPSP expected to provide to customers as evidence of PCI DSS compliance? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0024 / FAQ 1576: What information are TPSPs expected to provide to customers? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0100 / Data Security Essentials for Small Merchants: Guide to Safe Payments, Version 3.0 / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-15 against canonical digest

d1e65b27ee3081cb982599418fd7810486fecb37b807d81ecfb733e32e475916. Educational content, not a compliance determination.

Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.