

YOUR PAYMENT PROCESSOR HANDLES THE TRANSACTION. NOT EVERY RESPONSIBILITY.

A provider can perform the payment activity. The merchant still needs to understand the page, device, people, configuration, evidence, and response work surrounding it.

PRACTITIONER POSITION

Provider use should be described as an exact service and responsibility model, not as a transfer of PCI DSS itself. A merchant should obtain current provider evidence, confirm that the consumed service is covered, identify provider, customer, and shared activities, and preserve the configuration and operational records that support its own claims. A compliant provider can materially reduce exposure and effort. It cannot establish the merchant's eligibility, scope, implementation, or validation result by logo alone.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A member says the processor handles PCI. The processor hosts the payment form, but the member controls the website, DNS, administrator accounts, plugins, customer support, refunds, emailed links, and the webhook that receives transaction status. The provider performs important work. The merchant still operates several paths that can affect the payment journey.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The provider name appears where an exact service should be identified.
- A compliance badge substitutes for an AOC, covered-service description, or responsibility record.
- Customer configuration and monitoring duties are absent from the operating calendar.
- A provider or feature change does not reopen the merchant's payment story.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Inventory the exact service, account, feature, integration pattern, environment, and payment journey consumed-not only the corporate provider relationship.

Ask for current evidence in the appropriate official form and verify that it covers the relevant service.
Preserve limitations, dates, locations, and customer conditions.

Write provider, customer, and shared duties in verbs: configures, approves, patches, monitors, scans, tests, investigates, retains, notifies, and supplies evidence.

Assign a merchant owner to monitor service, evidence, responsibility, configuration, and incident changes.
Outsourcing execution does not outsource awareness.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 What exact service and feature does the business consume?

02 What current evidence shows that service is within the provider's assessed scope?

03 Which duties remain with the merchant or are shared?

04 Who notices when evidence, service behavior, or configuration changes?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect contracts, service descriptions, current AOCs, responsibility information, configuration, and merchant workflows.

02 / MAP

Join every payment activity to provider, merchant, or shared execution and evidence.

03 / EXPLAIN

State the narrow claim the provider evidence supports and the merchant duties it does not remove.

04 / REDUCE

Remove unused features and direct data paths; correct unclear service coverage and unowned customer responsibilities.

05 / PROVE

Retain current provider evidence, responsibility records, merchant configuration evidence, completed duties, and change monitoring.

THE LINE WORTH REMEMBERING

A PROVIDER CAN PERFORM THE ACTIVITY. THE RESPONSIBILITY SEAM STILL BELONGS ON THE MAP.

Use the Provider Question Card before accepting 'our processor handles PCI' as a complete answer.

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

fdd7696e6626cecb048c0c146d22d7fd1d92e6d380e11774a2d829a2068d3f45. 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.