

MAP THE INFRASTRUCTURE DEFERRAL LEAVES BEHIND

A TPSP can perform the control and handle the card data while your identity, deployment, integration, logging, support, and response infrastructure remains able to alter the security outcome.

PRACTITIONER POSITION

Deferral moves execution. It does not automatically remove connectivity, security influence, or customer responsibility. Infrastructure components may remain in PCI DSS scope when they are in the CDE, connected to it, or can impact its security, or when they perform residual customer duties around a TPSP-delivered service. The determination is fact-specific: identity and access, administration, CI/CD, source repositories, integration runtimes, secrets, DNS, network paths, customer-controlled pages and scripts, monitoring, exports, support, vulnerability management, incident response, and alternate channels must be evaluated against the actual architecture rather than included or excluded by category.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A company routes account data directly from the customer's browser to a validated provider and removes PAN from its application server. Its diagram then shows only the browser and the TPSP. Missing are the identity provider that grants console access, the repository and pipeline that change the payment page, the secrets store and API gateway that integrate the service, the DNS account that routes customers, the SIEM that receives provider events, the support tools that investigate failures, and the old telephone path. Raw card-data handling shrank. The security-influence map did not disappear.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The post-deferral scope diagram removes everything that does not store, process, or transmit account data without evaluating connectivity or security impact.
- Identity providers, privileged access, administrator workstations, source repositories, CI/CD, secrets, DNS, certificates, and network-control planes are missing from the influence analysis.
- API gateways, functions, webhooks, integration platforms, queues, logs, SIEM, backups, exports, analytics, and data lakes are assumed harmless because PAN should be tokenized or absent.
- Customer-controlled pages, scripts, mobile releases, support tools, chat, tickets, telephone paths, and error handling are not tested as ways to alter or bypass the intended provider boundary.

- Vulnerability management, change control, incident response, forensics, provider oversight, and annual evidence monitoring have no identified customer owner.
- The entity cannot explain why each residual component is included, excluded, or unresolved using current facts and evidence.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI DSS scope includes the CDE and system components connected to the CDE or that could impact its security. Provider-assisted designs can substantially reduce account-data exposure while leaving customer-managed systems capable of changing configuration, code, routing, authentication, monitoring, response, or an alternate data path.

PCI SSC FAQ 1312 makes the residual duty visible: the customer manages and oversees TPSPs, documents agreements and responsibilities, monitors status, and remains responsible for its own requirements. A TPSP-performed requirement remains in the customer's assessment scope, and missing provider evidence can prevent the assessor from finding it in place.

The right output is not a universal list of in-scope infrastructure. It is a reasoned topology. For every component, ask what it connects to, what it can change, which provider or customer activity depends on it, what data it receives, what failure or compromise could do, what evidence supports the conclusion, and which change reopens it.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which components administer, authenticate, authorize, deploy, configure, route, integrate, observe, support, or recover the TPSP-delivered service?
- 02 Which systems are connected to the CDE or could impact its security even though they should never receive account data?
- 03 Which logs, webhooks, exports, queues, backups, reports, analytics, tickets, chats, calls, or failure paths might receive more data than the intended design?
- 04 Who performs the customer's residual provider-management, monitoring, vulnerability, change, access, incident, and evidence duties?
- 05 What current fact and evidence support each component's included, excluded, separately covered, or unresolved disposition?
- 06 Which identity, code, configuration, service, provider, data-schema, or channel change automatically reopens the map?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Begin with the provider service and discover every customer and shared component that authenticates to, administers, changes, integrates, routes, monitors, supports, recovers, or can bypass it.

02 / MAP

Draw account-data paths and security-influence paths separately. Tag every component as CDE, connected, security-impacting, residual customer duty, separately covered, excluded with rationale, or unresolved.

03 / EXPLAIN

Write a fact-specific rationale for each disposition. Separate raw-data reduction from the residual scope and responsibility conclusions; do not infer either from the provider's compliance status.

04 / REDUCE

Remove unused administration, alternate channels, direct data paths, broad identities, unnecessary webhooks, excess logs and exports, unmanaged scripts, shared integrations, and provider features that enlarge the residual field.

05 / PROVE

Retain the topology, relationship facts, customer and provider responsibilities, test evidence, data schemas, negative-path results, owner, review date, and change triggers for every material component.

THE FIELD LAW

THE LINE WORTH REMEMBERING

OUTSOURCED EXECUTION CAN NARROW THE DATA PATH WHILE LEAVING THE SECURITY-INFLUENCE PATH INTACT.

Put the provider at the center of a blank page. Add every system that can authenticate, deploy, configure, route, integrate, observe, support, or bypass it. Now explain each line before erasing anything.

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](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

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

b68ec04a44cc76bf5369bba4a5e34241526dec0748f994110874a0422fd07818. 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.