

THE FIVE SYSTEMS EVERY SMALL MERCHANT SHOULD BE ABLE TO NAME

A small merchant does not need a hundred-page architecture package. It does need a current, explainable picture of the few systems that make payment possible or can affect it.

PRACTITIONER POSITION

Use five practical buckets as a discovery aid: customer payment entry points; merchant devices and webpages; provider services; administrative and support access; and networks, identities, or tools that can affect security. These are not PCI SSC scope categories and they do not decide applicability. They give a business owner a vocabulary for finding what exists before a qualified person or compliance-accepting entity determines what the facts mean.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A retailer lists two payment terminals as its complete environment. The discussion later reveals an ecommerce plugin, a tablet used for refunds, a vendor remote-support account, a router shared with guest Wi-Fi, and an employee mailbox receiving payment-link notifications. None of the discoveries proves a specific compliance result. Together they show why the original two-device story was incomplete.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The inventory contains only physical terminals.
- Webpages, virtual terminals, mobile devices, and refund workflows are missing.
- Provider administration and remote support are treated as invisible.
- The diagram cannot be reconciled to what employees actually do.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Name every customer entry point: terminal, reader, website, payment link, telephone workflow, virtual terminal, recurring system, donation page, and mobile event device.

Name the merchant-controlled devices and pages that host, launch, administer, support, or influence those entry points even when they do not intentionally store card data.

Name provider services by function and account. Include processor, gateway, ecommerce, hosting, managed IT, remote support, call, donation, recurring-billing, and other relevant providers.

Name administrative access and enabling infrastructure in ordinary language: who logs in, from where, using which device or identity, through which network, and with which recovery path.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Where can a customer begin a payment?

02 Which merchant-controlled device or page participates?

03 Which provider and administrator can change the journey?

04 Which diagram or list would become stale first after a business change?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Walk the business, website, invoices, phone scripts, events, support desk, and provider portals to identify the real payment estate.

02 / MAP

Group discoveries into entry points, merchant systems, providers, access, and security-influencing infrastructure.

03 / EXPLAIN

Describe what each item does, who owns it, and how it relates to a payment journey without deciding scope by category.

04 / REDUCE

Remove unused devices, accounts, plugins, paths, and shared arrangements that add complexity without business value.

05 / PROVE

Reconcile the list to current configurations, provider records, network observations, staff interviews, and change history.

THE LINE WORTH REMEMBERING

IF THE OWNER CANNOT NAME IT, THE ANNUAL FORM WILL NOT MAKE IT GOVERNED.

Complete the Payment Journey Sketch and see whether every device, page, provider, administrator, and connection has a name and owner.

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-0037 / FAQ 1252: PCI DSS applicability to system components / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0099 / Resources for Small Merchants / 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

6d0cbaa80e936eaae0cf7fcd1d61eb3d8f3a639e7f7e89a3791875716d51ebf5. 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.