

YOUR WEB DEVELOPER MAY BE PART OF YOUR PAYMENT-SECURITY STORY

The developer may never see a card number and still control code, credentials, scripts, hosting, or changes that can affect the payment journey.

PRACTITIONER POSITION

Payment responsibility is not limited to people who intentionally handle card data. An ecommerce merchant should understand who controls the payment page, redirect, iframe integration, scripts, plugins, hosting, DNS, deployment, administrator accounts, backups, logging, and incident escalation. Whether a particular developer, system, or activity is in PCI DSS scope is fact-specific. The business-owner action is simpler: document the access and influence first, then obtain qualified and program-specific direction instead of declaring the relationship irrelevant because payment processing is outsourced.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A Chamber member uses a hosted payment page. A freelance developer maintains the merchant website and can change the button, scripts, redirect destination, DNS, plugins, and hosting configuration. The processor receives card data, but the merchant has not documented the developer's access, change approval, account removal, security responsibilities, or incident contact path.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The developer is described as out of scope solely because the processor receives card data.
- Administrative accounts and deployment credentials are not inventoried.
- Third-party scripts and plugins can change without payment-impact review.
- The business has no retained record of who approved or deployed a payment-page change.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Inventory every party that can change the customer payment experience, including developers, agencies, hosting providers, plugin vendors, DNS administrators, managed IT, and ecommerce staff.

Record access type, purpose, environment, owner, approval, authentication, review, removal, logging, and emergency path. Avoid using job titles as technical boundaries.

Make payment-impact review part of ordinary website change. A design refresh, plugin, tag, redirect, CDN, form, checkout setting, or administrator change can matter even when the provider relationship is unchanged.

Confirm current SAQ eligibility and scanning direction with the compliance-accepting entity. Do not use this article to select a form or target population.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Who can change the payment page, redirect, scripts, hosting, or DNS?

02 Which accounts and devices permit that change?

03 How is a payment-impacting change approved and evidenced?

04 Who removes access and preserves records when the relationship ends?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

List people and providers with code, content, hosting, DNS, script, plugin, deployment, and administrator capability.

02 / MAP

Connect every capability to the payment journey, access path, change record, owner, and incident contact.

03 / EXPLAIN

Describe the security influence without claiming that influence alone decides every PCI DSS requirement.

04 / REDUCE

Remove unused accounts and plugins, narrow privileges, separate duties where practical, and simplify the payment-page design.

05 / PROVE

Retain access reviews, authentication evidence, code and configuration history, approvals, monitoring, and tested removal.

THE LINE WORTH REMEMBERING

NO CARD DATA IN THE DEVELOPER'S HANDS DOES NOT MEAN NO PAYMENT-SECURITY INFLUENCE IN THE DEVELOPER'S ACCOUNT.

Add every website and payment administrator to the Payment Journey Sketch, then ask who can change what today.

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-0016 / FAQ 1588: SAQ A eligibility criteria for scripts / 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](#)
- WACK-SOURCE-0102 / FAQ 1604: ASV scans for SAQ A redirect and embedded-payment-page merchants / 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

a549f37e831077c8c0b115a33f8b4e0f8661e0982cb005b21a2f264af27cc605. 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.