

REDUCE CARD-ISSUING SCOPE WITH LITHIC

Lithic can present card details without sending them through your servers. That useful boundary exists only for the exact issuing experience, configuration, and data path you can prove.

PRACTITIONER POSITION

A correctly implemented Lithic Embedded Card UI can reduce where issued-card PAN, CVV, and expiration data enter a customer's environment because the browser requests those details directly from Lithic and displays them in a Lithic-hosted iframe. The customer backend still creates a short-lived embed session, and the customer still operates the page, identities, integration, administration, deployment, monitoring, support, and other issuing channels around it. Direct PAN APIs, PAN search, or full-PAN reporting represent different data paths and Lithic restricts relevant capabilities to customers with verified PCI compliance. This is an issuing architecture claim-not a merchant-acceptance shortcut-and the applicable PCI DSS scope and validation obligations remain fact-specific.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A card program replaces a customer-rendered PAN screen with Lithic's Embedded Card UI and declares its application stack out of scope. The browser does receive the card details inside the provider iframe, but the program has not documented session creation, target-origin controls, page integrity, administrative identities, mobile behavior, logs, customer support, exports, or the legacy API that can still retrieve card data. The new component may materially reduce exposure. The current statement is larger than the verified data path.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The scope rationale says 'Lithic is PCI compliant' but does not identify the precise Lithic product, environment, program, application, or card-detail experience.
- The team cannot show that PAN and CVV travel directly from Lithic to the browser-hosted iframe without entering customer servers, logs, telemetry, support tooling, or mobile bridges.
- Embed sessions, target origins, token lifetime, application authentication, and authorization to view a card are treated as implementation trivia rather than security controls.
- Direct card APIs, search-by-PAN capabilities, reports, exports, test tooling, or older card-detail screens exist outside the preferred embedded path.

- Customer-controlled pages, scripts, source repositories, CI/CD, identities, secrets, DNS, support processes, and administrative consoles are absent from the residual-infrastructure review.
- Lithic product documentation and provider compliance statements are treated as if they decide the customer's scope, requirement applicability, or validation method.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Lithic documents that its Embedded Card UI presents PAN, CVV, and expiration through an iframe and that the user's browser requests the data directly from Lithic, preventing those card details from touching the API client's servers. Lithic also requires server-side creation of a short-lived embed session with a target origin. Those are concrete product and data-path facts that can support a narrower architecture.

The reduction is integration-specific. Lithic's card API documentation states that PAN and CVV fields are available in production only to clients with verified PCI compliance, its search-by-PAN endpoint requires PCI compliance, and full PAN in certain reports is limited to PCI-compliant institutions. Activating one of those paths changes what the entity receives and can invalidate a conclusion based on the embed alone.

Lithic's terms describe provider PCI DSS responsibilities where Lithic handles cardholder data and corresponding customer security duties. PCI SSC guidance separately makes clear that an issuer may be subject to PCI DSS and that TPSP reliance does not transfer the assessed entity's responsibility to manage the relationship, identify responsibility, retain evidence, and meet its own duties. Product facts, provider validation, assessor judgment, and compliance-program direction must remain distinct.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which issuing journeys display, search, export, support, replace, activate, or otherwise expose card details, and which exact Lithic integration serves each one?
- 02 Can network observation prove that PAN, CVV, and expiration move directly between the user's browser and Lithic in the embedded journey without entering customer-controlled systems?
- 03 Who can create embed sessions, for which cardholder and card, with what authorization, target origin, expiration, logging, and abuse detection?
- 04 Which customer pages, scripts, mobile components, identities, deployment systems, secrets, DNS, administration, support, and monitoring can change or compromise the card-view experience?
- 05 Do any direct APIs, PAN searches, full-PAN reports, exports, logs, support tools, or fallback paths create a different PCI DSS boundary?
- 06 What current Lithic service evidence, responsibility information, customer operating evidence, and change triggers support the narrow claim?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory every Lithic program, environment, card-detail interface, embedded session issuer, direct API, search function, report, export, mobile path, administrative console, support workflow, and fallback.

02 / MAP

Trace issued-card data and security influence through the browser or device, Lithic iframe, session endpoint, customer application, identities, deployment systems, logs, support tools, and alternate paths.

03 / EXPLAIN

State exactly which data elements no longer enter which customer systems, which product facts support that statement, and which customer, shared, connected, or security-impacting responsibilities remain.

04 / REDUCE

Use provider-hosted display where appropriate, retire direct PAN retrieval and full-PAN exports that are not required, constrain session creation and target origins, sanitize downstream data, and remove obsolete paths.

05 / PROVE

Retain rendered and network-level tests, session and target-origin configuration, authorization tests, API and report entitlements, data schemas, logs, provider evidence, responsibility records, negative-path results, and change triggers.

THE FIELD LAW

THE LINE WORTH REMEMBERING

THE IFRAME CAN REMOVE CARD DATA FROM YOUR SERVER. IT CANNOT REMOVE YOUR OBLIGATION TO EXPLAIN THE SYSTEM WRAPPED AROUND IT.

Observe one normal card-view journey, one denied journey, and every alternate way staff or systems can obtain card details. If the data-path map changes when the iframe fails, the scope claim must include that path.

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-0025 / FAQ 1217: PCI DSS applicability to issuers / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0026 / Lithic Embedded Card UI / Lithic / [Open source](#)
- WACK-SOURCE-0027 / Lithic Terms of Service / Lithic / [Open source](#)
- WACK-SOURCE-0028 / Lithic Cards API / Lithic / [Open source](#)
- WACK-SOURCE-0029 / Lithic Search Card by PAN API / Lithic / [Open source](#)
- WACK-SOURCE-0030 / Lithic Reporting Suite / Lithic / [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

a6837dd26299ae2fe24e3898e491a25bed770235c47057e6cf767d65301e1337. 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.