

WHAT IS A CLAIMS LEDGER, AND WHY DO YOU NEED ONE?

A claims ledger is the connective tissue between what the assessed entity says, what the assessor tests, what the evidence actually covers, and what the report is allowed to conclude.

PRACTITIONER POSITION

My practitioner method uses a claims ledger as a governed register of material assessment assertions. 'Claims ledger' is practitioner vocabulary, not PCI SSC terminology and not a substitute for PCI DSS testing procedures or reporting templates. Each row states one bounded proposition about an identified subject, environment, population, and period; links that proposition to its authoritative basis and expected test; identifies the fact owner, implementation owner, evidence, exceptions, reviewer, and disposition; and records what would reopen it. The ledger is needed because assessment work otherwise tends to organize itself around artifacts and requirement numbers. Those are necessary, but they do not always expose the exact statement an artifact is being used to prove, the limits of that proof, or the difference between entity representation and assessor conclusion.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An evidence repository contains a policy, a configuration export, a dashboard screenshot, a ticket report, and a sample list under one requirement folder. The control owner believes the folder proves the requirement. The assessor believes the evidence applies only to production servers during part of the assessment period. The report writer believes the result covers every in-scope environment. All three people are looking at authentic records. They are carrying three different claims because nobody wrote the claim as a controlled object before evaluating the evidence.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Evidence is named and uploaded before the team states the exact assertion, subject, boundary, population, and period it must support.
- One requirement row carries several materially different implementations, owners, environments, or frequencies without separating their claims.
- The assessed entity's representation, assessor testing result, practitioner recommendation, and compliance-accepting entity decision are blended into one status field.

- A document or screenshot is linked to many requirements, but each use lacks a specific relevance and coverage rationale.
- Exceptions and contradictory facts live in email or meeting notes rather than beside the claim they qualify.
- A new assessor or control owner cannot reconstruct why a conclusion was reached without asking the original team.
- Changes to scope, providers, populations, system components, evidence sources, or testing results do not automatically identify the claims that may need review.
- The final report contains a conclusion more precise or broader than the retained testing chain.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

The claims ledger turns assessment reasoning into inspectable work. The assessed entity can confirm the facts it represents. The assessor can connect the applicable testing procedure to a defined population, evidence set, exceptions, and result. Reviewers can see whether report language is supported without reverse-engineering a directory of files. A claim may remain pending, qualified, contradicted, or reopened; the ledger is valuable precisely because it preserves those states instead of forcing premature green.

A claims ledger is not an evidence inventory. One artifact can support several claims, and one claim may require several artifacts. The ledger records the relationship and the reason. It is also not a requirement checklist: a single requirement may create many claims across implementations, locations, control occurrences, provider/customer responsibility seams, or testing populations.

PCI SSC FAQ 1566 reinforces the practical evidence boundary: the assessor remains responsible for determining whether evidence is relevant to the assessment scope, directly related to the requirement, timely, and sufficient to support the assessment opinion. The ledger does not make that judgment automatically. It gives the accountable people a traceable place to make, review, and preserve it.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact proposition is this row asserting, and can it be proven false as well as true?
- 02 Which subject, environment, scope boundary, implementation, population, and time period limit the claim?
- 03 Which PCI DSS requirement and testing procedure provide the authoritative basis, and which language is practitioner interpretation?
- 04 Who owns the underlying fact, who performs the control, who represents it, who tests it, and who records the final disposition?
- 05 What evidence supports this claim, what does each artifact cover, and which exceptions or contradictory facts qualify it?
- 06 Which change, new evidence, missed occurrence, provider update, or review finding must reopen the claim?

ESCAPE THE WACK

01 / FIND

Extract material scope, applicability, implementation, operation, evidence, testing, and reporting statements from the engagement plan. Split compound statements until each row has one testable proposition.

02 / MAP

Join every claim to its subject, boundary, period, PCI DSS source, testing procedure, implementation owner, fact owner, population, evidence references, exceptions, related claims, reviewer, report destination, and reopen triggers.

03 / EXPLAIN

Write a short rationale that states why the evidence is relevant, direct, timely, and sufficient-or why the claim is still pending. Keep entity representation, assessor judgment, practitioner position, and organizational acceptance visibly separate.

04 / REDUCE

Retire duplicate assertions, stop using requirement folders as a substitute for reasoning, split claims with incompatible populations or owners, and resolve contradictions before drafting the final conclusion.

05 / PROVE

Select one final assessment result and trace it backward through report language, disposition, test, population, evidence, exceptions, owner representation, authoritative basis, subject, and period. Then change one input and confirm the affected claim reopens.

THE LINE WORTH REMEMBERING

EVIDENCE WITHOUT A BOUNDED CLAIM IS JUST AN ARTIFACT WITH AMBITION.

Download the Claims Ledger Starter and write the first ten material assertions before the next evidence request. If a row cannot name its subject, boundary, period, population, evidence, owner, reviewer, and reopen trigger, the assessment conclusion is still carrying hidden assumptions.

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-0013 / PCI SSC Document Library / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0015 / FAQ 1566: Use of evidence obtained outside the current assessment / 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

77018896167d4ec097d768ceda16a179aa394255780fc2f0e49fe7df88602c31. 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.