CHAINIT PAY

EXECUTIVE WHITE PAPER

CIT-PP-EWP-1.0

Provable Purchase

Verified Authorization and Evidence for Card Disputes

Author
Jodi Durst, President, ChainIT Pay

Executive summary

By the time a chargeback reaches an acquirer, the purchase may be weeks old. The merchant then has a short window to explain what happened using records scattered across checkout, payment processing, fulfillment and customer service systems.

Merchants need evidence they can retrieve, understand and submit within the applicable deadline. When the response costs more than the purchase, contesting the chargeback becomes an economic decision. Better evidence needs to begin with the transaction itself. [1,2]

Provable Purchase applies the ChainIT Transaction Truth Architecture to card purchases and their subsequent disputes. Its proposed dispute evidence profile connects a verified person or organization, the right to use the payment account, current authority and applicable compliance, the purchase approved, the instruction executed and the outcome recorded. It draws on ChainIT ID, ChainIT Org ID, the Authority and Compliance Protocols, ChainIT Pay, Pactvera and the platform's evidence records. [10,11,12,13]

Agent-initiated purchases make this connection especially important. A consumer may delegate a purchase without attending checkout. A business may authorize an employee to grant an agent limited purchasing authority. A useful record must establish the source and limits of that delegation and whether it supported the actual purchase when the instruction was released.

Existing authentication, network protections and transaction records remain valuable. ChainIT's contribution is the connected, verifiable evidence chain across those controls. The proposed Dispute Evidence Package would make relevant records available through participating acquirers, with disclosure tailored to the dispute.

That record can support a merchant that fulfilled its obligations. It can also establish that a transaction exceeded its authority or that a merchant failed to honor approved terms. Network rules, applicable law and the facts continue to govern the outcome. The commercial objective is measurable improvement in evidence completeness, response time and dispute economics.

This edition distinguishes platform foundations, published protocol architecture, the proposed dispute evidence profile and external dependencies. The proposed package is not represented as generally available or as a network-approved compelling-evidence format.

1 - The dispute problem in acquiring

A dispute becomes an operational problem when the merchant must connect records held by different systems. A payment approval can identify an accepted authorization request. An order record can describe the purchase. A carrier or service record can address fulfillment. The response must connect the relevant facts to the specific claim and arrive within the applicable deadline.

The cost extends beyond the disputed sale. Mastercard's 2026 Datos research forecasts 359 million annual chargebacks globally in 2029. Its updated cost analysis cites 2026 Javelin research reporting average US merchant costs of $82 internally and $46 in third-party fees per

chargeback, before lost goods or services. These are study averages, not a forecast for any particular merchant. [1]

Different disputes require different evidence. Third-party fraud concerns use without the cardholder's permission. First-party misuse concerns an improper fraud or unauthorized-purchase claim about a legitimate purchase, potentially arising from confusion or intentional abuse. A purchaser may also have a valid claim about delivery, defects, cancellation or a refund. Those legitimate claims must remain distinct from misuse. [4]

2 - Existing protections and the remaining evidence gap

Payment networks already provide meaningful authentication, dispute protection and evidence-sharing mechanisms. A connected purchase record should preserve and complement those protections.

Authentication and transaction confirmation

Eligible 3-D Secure authentication, including specified attempted-authentication flows, can protect merchants against fraud-dispute liability when the applicable conditions and submitted authentication data are satisfied. It does not resolve every issue involving delegation, commercial performance or non-fraud disputes. ChainIT evidence itself creates no network liability shift. [2]

Secure Payment Confirmation is designed to produce cryptographic evidence that a user confirmed transaction details. Mastercard's Agent Pay Acceptance Framework describes purchase-intent data and a dispute-relevant audit trail. EMVCo's draft agentic framework introduces services for managing consumer-authorized intent over time. These are useful inputs to the broader evidence chain. [5,6,7]

Network evidence programs

Under Visa's current CE3.0 rules, eligible history can span merchants and can include agentic-provider login IDs. Standard qualification generally uses two prior transactions within the applicable 120-to-365-day window and at least two matching elements, including IP address or device identification. Device ID and fingerprint are not independent factors. Acquirer access and processing restrictions apply. A customer new to one merchant may therefore have qualifying history available. [2]

Mastercard First-Party Trust has different requirements. Its published US guidance calls for a device factor, a delivery factor and a third distinct permitted element, shared during the transaction or dispute process. Protection depends on program eligibility. [4]

The remaining question is how those records connect to a verified principal, a valid delegation, current policy, the exact commercial instruction and attributable outcomes. Provable Purchase addresses that connected record, including cases where qualifying historical evidence is unavailable.

3 – “Connect the human, the account and the authority”

Identity, account entitlement and authority answer related but distinct questions. The proposed evidence profile must connect all three to the purchase. A verified person can still present a payment credential that the person is not entitled to use. A valid corporate account can still be used by an employee acting beyond delegated limits. [10,12,13]

Verify the person and establish the payment relationship

ChainIT ID supplies the individual identity foundation through authoritative-source verification, biometric and liveness controls, at the assurance level selected for the use case. ChainIT Org ID supplies the legal-entity foundation. For organizational activity, the record also identifies the verified person whose authority supports the action or delegation. An agent's workload authentication remains separate from that person's verification. [10,13]

The deployment must establish the relevant relationship to the designated account or payment credential using the evidence available from the issuer, wallet, processor, account holder or other qualified source. The record identifies the credential reference, the basis and scope of permitted use, and the source of that determination. Identity verification alone does not supply this entitlement. Sensitive account data remains subject to the participating payment environment's controls.

Principal	Authority source	What the purchase record connects
Individual	Authorized personal account use or a valid personal delegation	Verified person, designated credential, approved instruction and any delegated limits
Organization	Governing organizational authority and permitted delegation	Verified entity, authorized human, relevant corporate account, agent grant and current decision

Resolve the right to act and delegate

For a business, the Authority Resolution Pactvera (ARP) is the versioned organizational authority record. It identifies roles, powers, limits and approval requirements. The person granting authority to an agent must have the right to make that grant; the agent cannot receive greater authority than the supporting delegation permits. [10,13]

For an individual acting on personal assets, the applicable consumer profile establishes authorized account use and any personal delegation. An enterprise ARP is not automatically imposed on a consumer. The source of authority differs while the need to evaluate the proposed action remains. [12,13]

Evaluate applicable compliance and capacity

Applicable compliance requirements are evaluated under the selected policy using evidence current enough for the reliance event. A Compliance Decision VDT records that evaluation; it does not create authority or enlarge a grant. Required approvals, available spending capacity and current delegation status remain separate conditions of release. [10,11]

A recorded grant preserves what was delegated. Its present validity must be resolved when the proposed purchase relies on it. An unexpired login session or an agent's valid software credential cannot substitute for that evaluation.

4 - Govern the instruction and preserve its outcome

The purchase is represented by a canonical transaction object and its digest. Where human approval is required, the person approves understandable details corresponding to that object. For an autonomous purchase, the recorded mandate and current decision must cover the exact object. Material fields include the parties, payment reference, amount, currency, merchant, delivery instructions and relevant terms. Subscription or refund-policy evidence requires those terms and their version to be captured. [10,12,13]

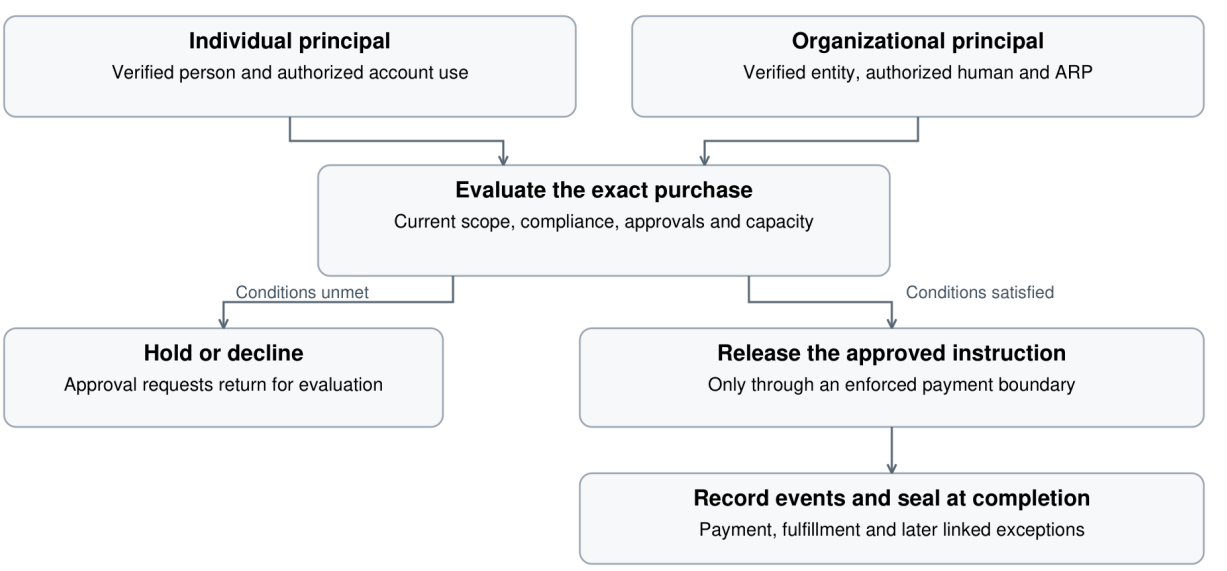


Figure 1 Authority sources converge on the purchase decision. The release branch applies only where an enforcement profile is implemented. Evidence accumulates through the lifecycle and is sealed at its defined terminal state. Sources [10,11,12,13].

Release only the approved instruction

At an implemented enforcement boundary, ChainIT Pay or a compatible partner adapter validates the single-use Execution Authorization Credential (EAC), reconstructs the transaction digest and applies the required release conditions. A material change requires a new evaluation

and any required approval. The boundary controls submission; issuer authorization, capture, settlement and fulfillment remain distinct events. [10,12]

Preserve state through completion

Pactvera and lifecycle Validated Data Tokens (VDTs) link decisions, approvals, payment events and fulfillment evidence. Valitorum seals a completed or otherwise terminal record under a defined completeness rule. Later refunds, returns and disputes are linked without rewriting that record, including through a Supplemental Valitorum where the profile supports it. [10,11,12,13]

Open transactions must remain answerable: an inquiry may arrive before settlement or delivery. The proposed profile therefore includes a dated current-state extract, with missing or pending events identified. Sealing establishes integrity of the preserved record; the accuracy of a source assertion still depends on its provenance and verification.

5 - Two illustrative purchase scenarios

These fictional examples combine platform foundations, published controls, proposed dispute packaging and deployment-specific integrations. They describe required behavior for a participating implementation, not a claim of universal production availability.

A consumer agent within a recorded budget

Dana has a verified ChainIT ID. In this configuration, a participating payment provider supplies evidence connecting Dana to a tokenized card credential she is entitled to use. The record retains the credential reference and the basis for that entitlement.

Dana grants a registered agent permission to purchase outdoor equipment from named merchants, up to $400 per purchase and $1,000 per month. The grant specifies her delivery address and excludes subscriptions. Her approval covers the understandable mandate and its enforceable parameters.

During the month, $600 has been spent and $100 is reserved for a pending purchase. The available capacity is $300. A proposed $280 tent purchase can proceed after the applicable authority, compliance, freshness and execution checks, leaving $20 available. A $350 proposal cannot proceed under that grant, despite being below the per-purchase limit.

Any permitted exception needs an independently authorized decision that explicitly addresses the monthly limit and its accounting. Biometric confirmation alone does not increase the budget. Approval of one exception does not silently expand the agent's standing grant. [10,13]

If Dana later questions the $280 charge, the proposed package connects the verified person and permitted credential use to the mandate, decision, submitted instruction and subsequent events. It can show what the recorded mandate permitted. It cannot by itself settle whether an ambiguous instruction matched Dana's expectations or whether the merchant delivered conforming goods.

An agent purchasing for a verified business

Northstar Manufacturing has a verified ChainIT Org ID. Its procurement director has a verified ChainIT ID and organizational authority to delegate defined purchasing activity. The company's payment arrangement establishes permitted use of the relevant corporate card credential.

Under the ARP, the director grants an agent authority to order approved supplies from designated merchants, subject to a $2,000 purchase limit and a $10,000 monthly limit. Before releasing a proposed $1,800 purchase, the controls evaluate the supporting organizational authority, current delegation, applicable compliance, available capacity and exact instruction. The record connects the company, the authorized human, the agent and the payment reference.

If the director's supporting authority is revoked and that change is effective and observable before the required release check, the payment is held or denied under the profile. A previously issued EAC cannot substitute for required current status. The implementation must declare its status-freshness bound and release cutoff; revocation does not recall an instruction already submitted. [10,11,12,13]

A later dispute can be assessed against the recorded authority chain and outcome. The same evidence may establish correct execution or identify an unauthorized purchase. The relevant liability and dispute rules still apply.

6 - Put the evidence into the dispute workflow

The proposed Dispute Evidence Package is a purpose-limited extract of the transaction record. It is designed for submission through a participating acquirer in a form appropriate to the actual claim. A readable account of the transaction should be available even when the issuer has no direct ChainIT integration. Machine-verifiable attestations and record references can accompany that account where the receiving workflow supports them.

The package would connect the case and payment references to the relevant identity-assurance result, account-use relationship, authority decision, displayed terms, approval, instruction and subsequent events. It would identify pending facts and missing evidence instead of treating an incomplete lifecycle as a completed outcome. Appendix A describes the proposed record contents.

Question in dispute	Relevant contribution	Evidence still required
Unauthorized purchase	Verified actor, permitted account use, approval and executed instruction	Applicable network eligibility and a reason-specific response
Agent exceeded its grant	Recorded mandate, supporting authority, current status, limits and decision	Review of contested instructions and any ambiguity or alleged misconduct
Goods or services not received	Approved delivery terms and linked fulfillment events	Attributable delivery, receipt, availability or usage evidence appropriate to the case

Question in dispute	Relevant contribution	Evidence still required
Cancellation or refund	Approved terms, cancellation event, credit instructions and payment references	Whether the required cancellation or credit actually occurred
Not as described or defective	Versioned description and terms, linked to the approved purchase	Evidence of actual condition, performance and any remedy

Disclose what the case requires

Raw biometrics, government identity records and unrelated personal information should remain outside ordinary merchant dispute responses. The package supplies the assurance and supporting evidence needed for the specific purpose. Network-required fields still control: a privacy-preserving assertion does not automatically replace required cleartext data. [2,10,11]

Authorized recipients, retention, verification access and submission deadlines must be defined for the deployment. Neither a seal nor a verification link makes an unsupported source statement true. The response should preserve source attribution and distinguish observed events, verified assertions and unresolved facts.

Support a fair determination

The record is neutral. It may establish that an authorized purchase was performed correctly, or that the merchant billed after cancellation. Applicable credit-card and consumer electronic-transfer rules use different authority and liability tests; a recorded mandate does not replace those rules or determine every question of consumer intent. [8,9]

Where records qualify for a network evidence program, they must be submitted through the program's required channel and format. Acceptance of additional ChainIT evidence, its weight and any resulting relief remain matters for the applicable process.

7 - Measure the commercial value

The proposed profile should be evaluated against the merchant's actual dispute workflow. The immediate opportunity is operational: capture evidence prospectively, connect it to the payment, and reduce the work required to prepare a timely and relevant response. Better information may also resolve an inquiry before it becomes a chargeback. The results must be measured.

A transparent handling cost illustration

Consider a hypothetical merchant receiving 100 formal chargebacks each month. Applying the published US averages of $82 in internal cost and $46 in third-party fees produces the illustration below. The chargeback count is an assumption; the averages are research inputs, not measured costs for this merchant. [1]

Illustrative input or result	Amount
Formal chargebacks per year	1,200
Internal and third-party handling cost per case	$128
Modeled annual handling expense	$153,600

This calculation excludes disputed principal, merchandise cost and recoveries. It does not estimate ChainIT savings or ROI. A pilot should measure the participating merchant's actual cost per case, then account for implementation, ongoing service cost and any checkout effect.

Keep monitoring relief separate from recovery

VAMP uses reported fraud plus disputes over settled Visa card-not-present transactions. The published US, Canada, Europe and Asia Pacific excessive-merchant criteria include a 1.5% ratio and at least 1,500 monthly events, with acquirer portfolio status also affecting treatment. Specified pre-dispute resolutions and CE3.0-qualified fraud records may be excluded, subject to data-extract timing. Recovery through ordinary representment is a separate result. The 100-case example alone does not establish merchant program eligibility. [3]

Evaluate one defined cohort

Measure	Evaluation method
Completeness and preparation time	Compare required evidence present and staff time per response
Timeliness and submission acceptance	Track deadlines met and responses accepted by the acquirer
Inquiry resolution and recovery	Separate pre-chargeback resolution from recovery by dispute condition
Monitoring treatment	Confirm specific exclusions using the applicable program records
Checkout and net economics	Measure completion, step-up abandonment and total operating cost

Use comparable transaction and dispute cohorts, document eligibility and selection effects, and allow cases to reach their relevant final outcome. A favorable decision in one case does not establish a general recovery rate.

8 - Deployment and the next commercial step

An institution should identify the integration mode before evaluating benefits. An evidence connection records and exports facts. An advisory connection evaluates a proposed action. An enforced connection can prevent submission through its controlled boundary. These modes offer different capabilities and must be described accurately. [13]

Status class	Scope in this publication
Platform foundation	ChainIT ID, ChainIT Org ID, ARP, ChainIT Pay, Pactvera, lifecycle VDTs and Valitorum as described in the companion publications
Published protocol architecture	Current authority and compliance decisions, capacity controls, EAC enforcement and execution-lifecycle controls; implementation and validation are specific to the deployment
Proposed dispute evidence profile	The Dispute Evidence Package, current-state inquiry extract, reason-specific presentation and mapping into network evidence workflows
External dependency	Payment-account entitlement evidence, processor and acquirer interfaces, issuer verification, program enrollment and network treatment of submitted evidence

Published architecture does not establish that every endpoint implements every control. Agent-initiated execution remains subject to the deployment scope described in the companion papers. A participating implementation must establish what is operational, what is being evaluated and which external parties supply or accept each record. No delivery timetable is implied by this publication. [10,11,12,13]

Define the operating limits

The enforcement profile must identify the release cutoff, status freshness, failure handling and permitted paths. Missing required evidence or an unavailable required status check cannot be silently treated as permission to release. A submission with an uncertain outcome must be investigated or reconciled using its existing reference before another payment is attempted. [10,11,12,13]

The evidence model does not eliminate coercion, deception, compromised enrollment or devices, ambiguous instructions, merchant nonperformance or residual exposure within declared freshness bounds. Transactions using a path outside the governed integration cannot be represented as having passed its controls.

Begin with one acquiring workflow

ChainIT Pay invites acquiring partners and selected merchants to evaluate the proposed dispute evidence profile in a defined pilot. We would select a transaction category, establish baseline

costs and evidence requirements, identify the participating payment path, and test how the resulting records move through the existing dispute process.

A successful evaluation should establish where connected evidence improves completeness, response time and economics, and what further integration is required. It should also show when the record supports the cardholder. That is how the evidence earns its value.

The purchase record should remain dependable after the transaction is questioned. By connecting the verified principal and authority to the approved instruction and attributable outcome, Provable Purchase gives merchants, acquirers and issuers a clearer basis for resolving the facts.

For a discussion of a defined pilot, contact ChainIT Pay through chainit.com.

Appendix A - Proposed evidence profile

The Dispute Evidence Package should be assembled from the existing transaction record and validated against the receiving workflow. The following categories describe the proposed profile; they are not a network-approved schema.

Record category	Required relationship or context
Case and transaction	Merchant and acquirer case identifiers; order and payment references; reason for the inquiry; relevant deadlines
Principal and account use	Identity-assurance result; verified entity and authorized human where applicable; payment-credential reference; source and scope of permitted use
Authority and policy	Personal mandate or organizational ARP and grant references; current status; applicable policy; compliance disposition; capacity and any exception approval
Terms and approval	Material purchase details; displayed terms and version; canonicalization version and digest; approval time and assurance; mandate-to-instruction correspondence
Execution and outcomes	Submitted instruction; authentication and issuer response references where available; capture, settlement, reversals, refunds and attributable fulfillment events
Integrity and disclosure	Seal or current-state reference; provenance; verification method; pending or missing facts; recipient scope and access controls; linked later exceptions

Lifecycle and adjustment rules

Card processing can include separate authorization, partial capture, multiple shipments, permitted adjustments and refunds. Each event must be linked to the approved purchase and its allowed transition. A material change outside the approved terms requires renewed evaluation and approval; the system must not preserve an old digest while substituting different material data. [10,12]

For human approvals and consumer mandates, preserve the understandable presentation alongside the enforceable parameters. A cryptographic match establishes correspondence with the recorded object. It does not prove that an ambiguous natural-language instruction was understood as the customer intended.

Key terms

ARP: Authority Resolution Pactvera, the versioned organizational authority record.

VDT: Validated Data Token, used to record attributable evidence, decisions and lifecycle events.

Canonical transaction digest: A hash of the transaction object under a defined encoding rule.

EAC: Execution Authorization Credential, a short-lived, single-use credential for one exact instruction and audience.

Pactvera: The governed agreement and execution container that binds parties, authority, terms, rules, consideration, actions and evidence.

Valitorum: The sealed record of a completed or otherwise terminal lifecycle under a defined completeness rule.

Supplemental Valitorum: A linked sealed record of a later exception that preserves the original record.

Definitions and control flows follow the companion Authority, Compliance and Transaction Truth publications. This proposed card-dispute profile does not amend those protocols. [10,11,12,13]

References and publication notes

Public sources were checked November 1, 2026. Citations support the specific factual statements identified in the text. Network rules vary by region and processing arrangement. The applicable rules and program documentation control individual cases.

[1] Mastercard. What is the true cost of a chargeback for businesses. Published April 30, 2025; updated June 8, 2026. Cites 2026 Datos forecasts and 2026 Javelin cost research.

[2] Visa. Visa Core Rules and Visa Product and Service Rules. October 24, 2026. Sections 4.1.23, 11.8.5.3 and 11.8.5.6; tables 11-29 and 11-32. The complete rules and applicable regional conditions control.

[3] Visa. Visa Acquirer Monitoring Program Overview. Official fact sheet, including the April 1, 2026 threshold change in footnote 5 and stated exclusions.

[4] Mastercard. First Party Trust program. US program information, including the definition of first-party fraud and published data requirements.

[5] W3C. Secure Payment Confirmation. Candidate Recommendation Draft, October 13, 2026. This is a developing specification, not a statement of universal browser support.

[6] Mastercard. Scaling agentic commerce with trust. October 14, 2025. Agent Pay Acceptance Framework, purchase-intent data and dispute-related audit records.

[7] EMVCo. Framework for secure interoperable and scalable card based agentic payments. September 1, 2026 announcement of the draft framework and Intent Services. Draft status is preserved in this paper.

[8] Consumer Financial Protection Bureau. Regulation Z section 1026.12. Special credit-card provisions, including the definition of unauthorized use and applicable liability conditions.

[9] Consumer Financial Protection Bureau. Regulation E section 1005.2. Definitions, including unauthorized electronic fund transfers; read with the official interpretations and applicable error-resolution rules.

[10] ChainIT. *Provable Authority*. CIT-PA-WP-7.0, September 1, 2026. Controls shared authority definitions, grants, decisions, credentials and execution flows.

[11] ChainIT. *Provable Compliance*. CIT-PC-WP-4.1, September 2026. Controls compliance evidence, policies, dispositions, freshness and disclosure.

[12] ChainIT. *Transaction Truth*. Executive White Paper CIT-TT-EWP-2.1 and Technical and Compliance Companion CIT-TT-TCC-2.1, September 17, 2026. Controls shared execution and settlement-evidence material.

[13] ChainIT. *Agentic Complete Commerce*. Executive White Paper CIT-AC-EWP-1.1, October 1, 2026. Consumer and organizational profiles, integration modes and agent execution.

Scope and intellectual property

This executive paper describes a proposed card-dispute application of the ChainIT architecture. It is not legal, regulatory, banking, accounting or security-certification advice. The model does not guarantee a dispute outcome, change network rules or establish that a particular record is admissible or conclusive. Responsible institutions retain

their own legal and regulatory obligations. ChainIT Pay performs regulated payment functions where appropriately authorized or through appropriately licensed partners.

Copyright 2026 Scientia Potentia Est II, LLC. All rights reserved. Recipients may access, retain and share an unmodified copy in its entirety for personal, informational or internal business purposes, with all notices retained and no distribution fee. Other reproduction, modification, publication or commercial use requires prior written consent. No patent, trademark, trade-secret or other intellectual-property license is granted beyond the permitted use of this publication.