# When Agents Pay: Permissions, Fraud and Liability in Payments M&A

*A Transaction and Control Framework for Delegated Authority, Agent Identity, Fraud Allocation and Post-Deal Integration*

**Authored by Chennakeshav Adya**

Independent Researcher

September 2026

---

## Abstract

*AI agents can search, negotiate and initiate payments for consumers and businesses. This capability changes the evidence surrounding a payment. A conventional checkout often assumes that a person is present, sees the final amount and performs an authentication step. An autonomous flow can separate intent, cart formation, credential access, authentication and execution across several systems and legal entities. The resulting value depends on whether the combined system can prove who authorised what, within which limits, for which merchant, at what time and with which payment instrument.*

*This paper develops a transaction and control framework for acquisitions of agentic-payment platforms, payment orchestration providers, wallets, fraud systems and commerce infrastructure. It distinguishes agent identity from user identity, permission from payment authorisation, transaction authenticity from lawful authority, and technical evidence from legal liability. It maps the roles of shopping agents, credential providers, merchants, processors, networks, issuers, acquirers and trusted consent surfaces. It then connects mandates, tokens, authentication, fraud controls, disputes, chargebacks, consumer protection, anti-money-laundering obligations, data protection and operational resilience to unit economics and enterprise value.*

*The analysis draws on current specifications and official material from payment networks, Google's Agent Payments Protocol project, the FIDO Alliance, regulators, central banks, standards bodies and financial-crime authorities.[1][2][3][4][5][6][7][8][9][10] These sources describe emerging mechanisms for agent recognition, verifiable intent, scoped credentials and interoperable payment controls. They also confirm that existing payment, consumer, data, financial-crime and operational-resilience obligations continue to apply according to product, role and jurisdiction.*

*A hypothetical acquisition illustrates a payment platform processing USD 4.0 billion of annual gross payment value. Every volume, conversion, loss, fee, cost, probability, multiple and valuation amount is a management assumption created solely to demonstrate the framework. None is a forecast, benchmark or valuation opinion.*

*The paper concludes that a buyer should value an agentic-payment platform as an evidence system attached to an operating payment business. Technical novelty deserves value only when authority is reproducible, credentials are scoped, controls are deterministic, disputes are supportable, liability is bounded and economics survive fraud and integration stress. Six figures and seven tables convert that conclusion into a diligence plan, liability map, unit-economics bridge, valuation method, transaction protections and 180-day programme.*

*Payments, consumer-protection, data, competition, artificial-intelligence, anti-money-laundering, sanctions, tax and corporate-law requirements vary by role and jurisdiction. Qualified specialists should*

*determine the rules and transaction consequences that apply. This paper provides general information and does not provide legal, regulatory, accounting, tax, investment or credit advice.*

**JEL Classification:** G21, G23, G34, K12, O33

**Keywords:** agentic payments, delegated authority, payment fraud, liability, M&A, digital identity, tokenisation, transaction controls

## 1. Define the acquisition decision

The investment question is whether the target owns a repeatable system that converts delegated intent into authorised, accepted and collected payments with bounded loss. The buyer should avoid valuing an agentic interface as though it were the payment business. Value arises from the complete chain of authority, identity, credentials, merchant acceptance, processing, fraud control, dispute evidence, settlement and customer outcomes.

The diligence perimeter should include every entity and service that influences the transaction. A shopping agent may assemble a cart, a trusted surface may collect consent, a credential provider may release a token, a merchant may accept the order, and a processor, network, issuer and acquirer may authorise and settle the payment. A failure at any interface can reduce conversion, increase fraud, create liability or interrupt cash.

The board should define the precise decision before diligence begins. It should state which products, rails, jurisdictions, licences, customer types, technology rights, network relationships and data assets support the price. It should also define which future capabilities remain contingent. A protocol demonstration, memorandum of understanding or pilot cannot support the same value as production transactions that reconcile to merchant delivery, dispute outcomes and collected revenue.

The proposed unit of value is an agent-initiated payment whose authority, checkout, credential, processing result, fulfilment and cash can be reconstructed. Portfolio metrics should aggregate only transactions that meet the same evidence standard.

## 2. Define an agent-initiated payment precisely

An agent-initiated payment is a transfer in which software acting under delegated authority performs a material part of product selection, checkout formation, payment-instrument selection, authentication or execution. The definition should distinguish assistance from autonomy. A conversational interface that suggests a product before a human completes checkout creates different risk from an agent that purchases without contemporaneous human presence.

The buyer should classify flows by authority mode, payment rail and execution channel. Authority may be specific to one checkout, open within a budget and merchant set, recurring, event-triggered or revocable. Rails may include cards, account-to-account transfers, wallets, real-time payments or digital assets. Execution may occur through a merchant API, browser automation, a commerce protocol or agent-to-agent exchange.

The technology stack should be mapped from instruction to settlement. Models may interpret intent, compare products or choose a payment method. Deterministic services should enforce spend limits, merchant restrictions, credential scope, nonce freshness, authentication and policy. The AP2 specification states that verification responsibilities should execute in deterministic code even where an agent participates in the wider flow.[1]

Marketing language should not define the perimeter. The diligence team should reproduce sampled transactions and identify the exact point at which human intent becomes a machine-enforceable instruction.

## 3. Map participants, roles and dependencies

Agentic commerce adds roles to an already distributed payment chain. AP2 describes shopping agent, credential provider, merchant, merchant payment processor and trusted surface roles.[1] Network implementations introduce agent registration, tokenisation and scheme controls.[3][4] A target may perform several roles or delegate them to vendors.

The buyer should create a legal-entity and responsibility map. For each role, it should identify the service, contracting party, licence, regulated activity, data processed, decision authority, control owner, revenue, cost, indemnity, insurance and failure consequence. Where one entity performs several roles, governance should prevent a commercial incentive from overriding an independent control.

Delegation requires an explicit chain. A platform may rely on an identity provider, wallet, cloud service, model provider, fraud vendor, token service, acquirer and network. The buyer should test whether each delegation is contractually permitted, technically observable, operationally supported and transferable on change of control.

Concentration should be measured by economic dependency and substitutability. A nominally multi-provider platform can still depend on one network, credential provider or merchant integrator for most volume. Replacement time, certification, customer consent and data portability should enter both valuation and integration planning.

## 4. Build the authority stack

Permission is not one event. A robust authority stack connects the user, agent, instruction, checkout, credential, merchant, amount, time and execution. Each layer should have an issuer, verifier, scope, expiry, revocation mechanism and durable audit record.

The buyer should distinguish general intent from transaction authority. An instruction such as “book a suitable hotel under USD 1,000” does not establish the final merchant, dates, cancellation terms, currency or card. The system should transform the instruction into constraints, assemble a checkout and obtain the level of approval required by risk, law and product design.

Open mandates support bounded autonomy. Closed mandates bind approval to a specific checkout and amount. AP2 uses checkout and payment mandates with signed receipts to create evidence across participants.[1][2] Network approaches similarly emphasise registered agents, tokenised credentials and verifiable user intent.[3][4]

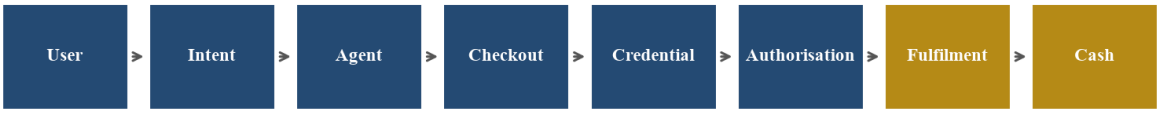
**Table 1. Authority-stack diligence matrix**

| Layer | Core question | Required evidence | Failure consequence |
|---|---|---|---|
| user identity | who is delegating | authentication, account and device evidence | impersonation and dispute |
| agent identity | which software is acting | registration, certificate, key and owner | malicious-bot acceptance |
| intent | what outcome is permitted | signed instruction, limits and expiry | excessive or unintended purchase |
| checkout | what is being bought | merchant-signed cart, price and terms | substitution or price manipulation |
| credential | which instrument may pay | scoped token, device binding and issuer decision | credential misuse |
| execution | what occurred | processor response, nonce and timestamp | replay or duplicate payment |

| Layer | Core question | Required evidence | Failure consequence |
|---|---|---|---|
| fulfilment | what was delivered | acceptance, delivery and refund evidence | chargeback and merchant loss |

*Proposed framework; applicable requirements depend on the product, rail and jurisdiction.*

**Figure 1. Proposed authority-to-cash evidence chain**




*Each transition requires a named verifier, durable record and exception path.*

## 5. Reconstruct consent and mandates

Consent should be specific enough to guide execution and durable enough to support a later dispute. The diligence team should inspect how the user sees the instruction, checkout, amount, merchant, instrument, timing and material terms. It should identify what is signed, by whom, using which key, on which trusted surface and with which revocation rights.

The interface matters because model output can differ from user understanding. A natural-language request may be ambiguous. The system should surface assumptions that change economic or legal effect, including subscriptions, cancellation rights, foreign exchange, tips, delivery windows and non-refundable terms. High-risk or out-of-policy changes should return to a human approval step.

Mandates should be versioned, scoped and linked. AP2 binds payment authority to a checkout and provides receipts that can be verified during a dispute.[1] The buyer should test key rotation, expiry, nonce use, replay prevention, selective disclosure, revocation and archival retrieval. It should also test whether a mandate can be reused across merchants, carts, amounts or credentials.

The target should retain evidence for the applicable dispute and regulatory period. A cryptographic object has limited value when keys, schemas, verifier software or contextual records cannot be reproduced after the transaction.

## 6. Separate agent recognition from user identity

Merchants need to distinguish approved commerce agents from crawlers, malicious bots and unauthorised automation. Visa’s Trusted Agent Protocol describes signed mechanisms for agent recognition, consumer recognition and payment containers.[5][6] Mastercard’s Agent Pay materials describe registered agents, tokenised credentials and verifiable intent.[3][4]

Agent recognition confirms the software participant and its trust framework. It does not prove that a particular user authorised a particular purchase. User identity, account state, device, authentication and mandate evidence remain separate. The buyer should reject architectures that collapse these questions into one “trusted agent” flag.

The diligence sample should test unknown agents, expired certificates, revoked agents, key rotation, replay, altered headers, proxying, credential substitution and legitimate agents with out-of-scope instructions. Merchant controls should fail safely and record a reason that can be reconciled to conversion and fraud outcomes.

Registration economics also matter. Certification, network onboarding, monitoring and support can create defensibility or cost. The buyer should verify whether registrations transfer on change of control and whether the target's role is replaceable by a common network or cloud service.

## 7. Bind transaction context and prevent replay

A payment request should be bound to the merchant, checkout, amount, currency, credential scope and freshness window. Without binding, an attacker may relay a valid approval to another merchant, alter the cart or reuse a signed object. HTTP Message Signatures and network protocols provide technical building blocks for message integrity and origin verification.[7][5]

The buyer should reconstruct how nonces, timestamps, audience restrictions, request targets, content digests and keys are verified. It should identify which participant rejects an invalid object and whether downstream systems can distinguish a cryptographic failure from an ordinary decline.

Idempotency and duplicate control require equal attention. Agents may retry after timeout, invoke several providers or continue after a delayed response. The system should prevent multiple captures, duplicate fulfilment and inconsistent receipts. Reconciliation should connect each instruction to one economic outcome or a documented reversal.

Failure tests should include clock drift, network interruption, partial fulfilment, price changes, expired inventory, currency conversion and authentication challenges. The target should demonstrate deterministic rollback and customer communication rather than relying on a model to improvise recovery.

## 8. Test authentication and payment controls

Strong customer authentication, risk-based authentication, tokenisation, device binding and payment passkeys can reduce risk when correctly integrated. Their legal and scheme effects depend on the rail and jurisdiction. The EBA and ECB report that strong customer authentication remains effective against fraud types it was designed to address, while fraudsters increasingly manipulate payers.[11]

The buyer should examine the decision sequence for human-present and human-not-present flows. It should record when authentication occurs, what transaction data the user sees, what exemptions apply and which participant bears the result. A model recommendation should not silently replace a mandatory authentication or policy decision.

Authentication evidence should reconcile to authorisation, clearing, settlement and dispute data. Pass rates alone are incomplete. The board should see conversion, false decline, fraud, challenge abandonment, support cost and liability by method and cohort.

**Table 2. Control test for agent-initiated payments**

| Control | Test | Evidence | Valuation relevance |
|---|---|---|---|
| agent registration | valid, revoked and unknown agent | certificate and decision log | addressable accepted volume |
| mandate | amount, merchant and expiry boundary | signed object and receipt | dispute defensibility |
| credential scope | reuse and substitution attempt | token and issuer response | fraud and network acceptance |

| Control | Test | Evidence | Valuation relevance |
|---|---|---|---|
| authentication | present and autonomous flows | challenge and exemption evidence | conversion and liability |
| replay defence | duplicate nonce and delayed request | deterministic rejection | loss containment |
| idempotency | timeout and retry | single capture and fulfilment | customer and merchant outcome |
| revocation | user, agent and credential withdrawal | propagation time and denial | tail-risk duration |

*Proposed test catalogue; scheme and legal requirements prevail.*

## 9. Build an agentic-fraud taxonomy

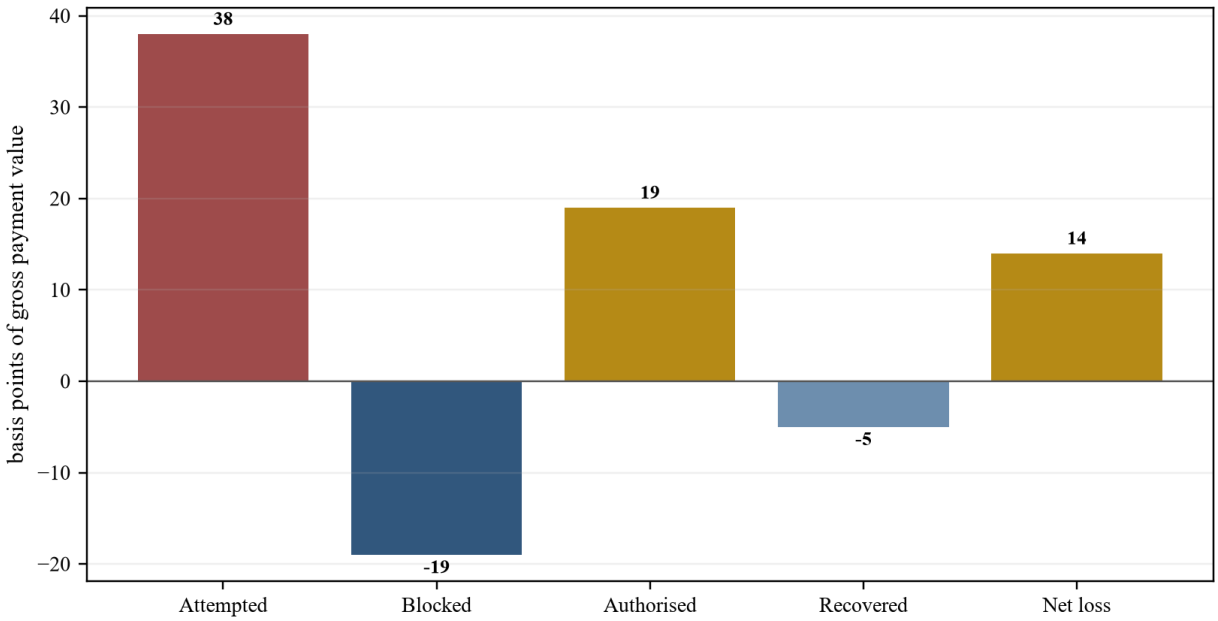
Agentic payments inherit conventional account takeover, credential theft, merchant fraud and social engineering. They add failures involving instruction manipulation, malicious tools, prompt injection, agent impersonation, mandate tampering, cart substitution, model error and unauthorised delegation. The buyer should distinguish attack, accident, control failure and commercial dispute because prevention and liability differ.

Fraud can enter before payment. A malicious product page may manipulate the agent, a compromised tool may change delivery details, or a fake merchant may present a plausible checkout. Fraud can also enter after authority through credential misuse, replay, duplicate execution, non-delivery or refund abuse.

The target should map each fraud type to preventive, detective and recovery controls. It should show which signals were available at decision time, what action was taken, who owned the loss and how quickly the system learned. Fraud labels should be independently reviewed because reclassifying losses as customer dispute or merchant error can overstate model performance.

Attack adaptation should enter valuation. A control that performed well during a small pilot may deteriorate when transaction volume and attacker attention increase. Stress testing should include common-provider compromise and coordinated abuse across agents and merchants.

**Figure 2. Hypothetical agentic-payment loss funnel**




*Wholly hypothetical basis-point losses on gross payment value; amounts demonstrate reconciliation only.*

## 10. Reconstruct liability by rail and jurisdiction

Liability follows legal definitions, scheme rules, contracts and facts. The technical presence of a signed mandate does not determine the legal outcome by itself. The buyer should map consumer, business, merchant, issuer, acquirer, processor, network, wallet, credential-provider and agent-platform exposure for each supported flow.

In the United States, Regulation E establishes rights, liabilities and error-resolution rules for covered electronic fund transfers. Its definition of unauthorised transfer and rules on consumer liability require fact-specific analysis of actual authority, access devices and benefit.[12][13][14] An agent authorised within limits creates a different question from a fraudster using stolen credentials or an agent exceeding its mandate.

In the European Union, PSD2, the developing PSD3 and Payment Services Regulation framework, strong customer authentication and fraud-allocation provisions shape payment-provider exposure.[15][16] The United Kingdom combines payment-services rules with reimbursement and consumer-outcome requirements.[17][18] Other jurisdictions apply their own retail-payment, stored-value, data and consumer regimes.[19][20]

The buyer should create a legal position paper for every material product and geography. It should avoid treating “user approved the agent” as a universal waiver. Consumer protections, scheme allocation, negligence standards and contractual limits may restrict that position.

## 11. Build dispute-grade evidence

Disputes test whether the platform can reproduce the transaction as experienced by each participant. The evidence set should include the user instruction, mandate, trusted-surface presentation, merchant-signed checkout, credential scope, authentication, agent and key status, processor messages, fulfilment, communications, refunds and receipts.

AP2 describes mandate and receipt verification for disputes, including verification of checkout and payment hashes.[1] The buyer should run historic and synthetic disputes through the complete retrieval process. Evidence should remain available after key rotation, schema change, vendor exit and employee departure.

The dispute operation should record reason code, owner, deadline, amount, provisional credit, evidence submitted, result, recovery and root cause. Chargeback win rate should be segmented by transaction type and evidence completeness. A high win rate can still conceal poor customer outcomes or delayed cash.

Legal privilege, retention and privacy require design. The evidence room should preserve necessary facts without exposing unrelated personal data or secrets. Access, export and deletion should be controlled and auditable.

## 12. Rebuild complete unit economics

Agentic-payment economics should begin with settled value and collected revenue, then deduct network and processing expense, fraud, disputes, refunds, incentives, authentication, agent-registration cost, customer support, compliance, infrastructure and partner shares. Gross payment value does not establish enterprise value.

The hypothetical case processes USD 4.0 billion of annual gross payment value at a gross take rate of 42 basis points. It assumes 14 basis points of processing and network cost, 9 basis points of fraud and disputes after recovery, 4 basis points of incentives, 3 basis points of agent and authentication cost and 2 basis points of direct support and compliance cost. These assumptions produce 10 basis points, or USD

4.0 million, of contribution before central technology, sales, tax and capital cost. They are methodological assumptions only.

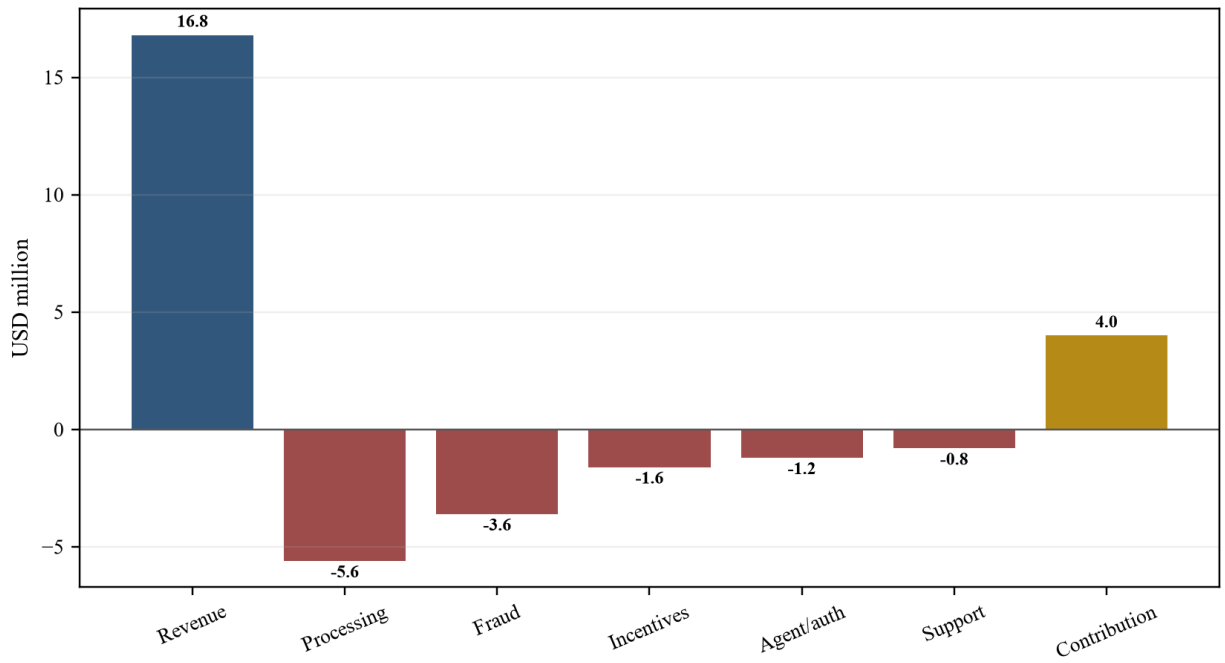
Economics should be segmented by merchant, agent provider, rail, region, credential type, authentication path and cohort. A new autonomous flow can raise conversion while producing higher dispute and support cost. The buyer should compare matched populations and recognise the time required for fraud and chargebacks to mature.

**Table 3. Hypothetical annual agentic-payment economics**

| Item | Basis points | USD million |
|---|---|---|
| gross payment value | 10,000 | 4,000.0 |
| gross revenue | 42 | 16.8 |
| processing and network | (14) | (5.6) |
| fraud and disputes | (9) | (3.6) |
| incentives | (4) | (1.6) |
| agent and authentication | (3) | (1.2) |
| direct support and compliance | (2) | (0.8) |
| contribution before central cost | 10 | 4.0 |

*Wholly hypothetical USD millions and basis points; the table is not a market benchmark.*

**Figure 3. Hypothetical contribution bridge**




*Wholly hypothetical USD millions; central cost, tax and capital requirements remain outside the displayed contribution.*

## 13. Measure conversion and false-decline economics

Merchants may block unknown automation to protect inventory, systems and customers. Trusted-agent recognition can recover legitimate demand, while poorly calibrated controls can admit fraud or reject valuable customers. The buyer should measure both sides of the decision.

Conversion should be decomposed from agent visit through product availability, checkout, credential release, authentication, authorisation, fulfilment and settlement. Every loss point should have a reason

code. A higher checkout rate can be offset by cancellations, duplicate orders, refunds or lower contribution.

False declines require verified counterfactuals. Manual review, subsequent successful payment, issuer feedback and matched cohorts can provide evidence. The analysis should distinguish merchant blocking, agent verification failure, credential denial, authentication abandonment and issuer decline.

Commercial forecasts should price merchant adoption and control quality separately. A protocol may be available while merchant integration, network recognition or consumer trust remains limited. Only implemented and evidenced conversion improvements should enter proven value.

## 14. Reconcile fraud, chargebacks, refunds and reserves

Loss reporting should reconcile attempted fraud, prevented fraud, authorised fraud, unauthorised fraud, merchant dispute, non-delivery, refund, chargeback, recovery and write-off. Definitions should be stable across periods and agree with network, processor, merchant and ledger records.

Reserve timing matters. Fraud can emerge quickly while disputes and chargebacks mature later. Growth can therefore improve current revenue before the full loss cohort develops. The buyer should build transaction vintages by authorisation month and follow them through final dispute status.

Contractual allocation should agree with observed practice. A processor may have indemnity rights that are difficult to collect. A merchant reserve may be insufficient or trapped. Network fines, monitoring programmes and remediation cost should be separated from transaction loss.

**Table 4. Loss and liability reconciliation**

| Event | Operational label | Cash owner | Evidence needed |
|---|---|---|---|
| stolen credential | unauthorised payment | issuer or provider subject to rules | access, authentication and fraud facts |
| agent exceeds limit | authority breach | fact-specific | mandate, revocation and presentation |
| altered checkout | transaction tampering | participant control owner | signed cart and hashes |
| duplicate execution | processing error | service causing duplicate | idempotency and capture logs |
| non-delivery | merchant dispute | merchant subject to scheme | fulfilment and communication |
| model mis-selection | service failure | agent platform subject to contract | instruction, ranking and disclosure |
| social engineering | manipulated payer | jurisdiction-specific | communications and authentication |

*Proposed reconciliation; transaction-specific facts and rules determine final allocation.*

## 15. Test data rights, privacy and purpose

Agentic payments combine identity, preferences, product searches, location, credentials and transaction history. The buyer should map each data element to source, lawful basis, purpose, recipient, retention, model use, transfer and deletion. Consent to purchase does not automatically authorise unrelated profiling or model training.

Selective disclosure can reduce exposure. Protocols can disclose only constraints required by a verifier, while tokens can avoid sharing primary credentials. The buyer should test whether production architecture follows that principle or copies complete instructions and credentials across vendors.

Data rights should survive the transaction. Contracts need access, audit, portability, security, incident notice, subcontractor and exit provisions. A target may depend on behavioural data that a partner can withdraw or that cannot lawfully transfer after change of control.

The valuation should include remediation and revenue loss where current personalisation depends on unsupported data use. Privacy engineering and reliable deletion are operating capabilities, not policy documents.

## 16. Apply financial-crime and sanctions controls

Automation does not remove obligations to understand customers, merchants, transactions and counterparties. The Financial Action Task Force's digital-identity guidance supports risk-based use of digital identity while emphasising governance and assurance.[21] FinCEN, OFAC and national authorities provide requirements and guidance relevant to money laundering, sanctions and suspicious activity.[22][23]

The buyer should identify which entity performs onboarding, screening, monitoring, investigation, reporting and recordkeeping. Agent and merchant identity can change the available signals, while rapid autonomous execution can shorten the time for intervention.

Controls should cover agent-provider ownership, merchant category, beneficiary, geography, device, credential, product, velocity and linked behaviour. Model alerts should feed a governed case process with human accountability. Sanctions controls need timely list updates, payment blocking and escalation.

Cross-border and digital-asset flows require separate analysis. The transaction team should avoid extending a domestic card-control conclusion to real-time transfers or blockchain settlement without rail-specific evidence.

## 17. Assess technology, resilience and third parties

The platform should continue to enforce authority during model, network and vendor failure. Architecture should separate probabilistic interpretation from deterministic policy and payment execution. Critical controls need explicit inputs, versioning, testing, monitoring, rollback and incident ownership.

The buyer should test cloud-region loss, key-service outage, identity-provider failure, model unavailability, network timeout, corrupted policy, delayed revocation, compromised tool and merchant API change. Recovery should preserve transaction state and prevent duplicate execution.

Third-party services should enter a complete register linked to contracts, data, keys, controls, service levels, concentration and exit. The Basel Committee's operational-resilience and third-party principles provide useful lenses where relevant.[24][25] NIST's AI and cybersecurity frameworks provide complementary control structures.[26][27]

**Table 5. Technology and third-party evidence matrix**

| Capability | Strong evidence | Weak evidence | Transaction response |
|---|---|---|---|
| policy enforcement | deterministic service and tests | prompt-only instruction | remediation condition |
| keys and signatures | managed lifecycle and rotation | shared unmanaged secrets | closing gate |
| state and idempotency | durable transaction state | retry without control | loss reserve |
| model change | versioned approval and rollback | silent production update | integration hold |
| vendor continuity | tested alternative and exit | single opaque provider | value deduction |

| Capability | Strong evidence | Weak evidence | Transaction response |
|---|---|---|---|
| incident response | rehearsed cross-party playbook | informal escalation | funded programme |
| evidence retention | reproducible after change | transient logs | dispute deduction |

*Proposed matrix; materiality determines test depth.*

## 18. Value the platform by evidence layer

Value should be divided into proven operating value, evidenced expansion and contingent option value. Proven value comes from production transactions with reproducible authority, stable fraud and dispute cohorts, accepted network and merchant operation, transferable rights and collected contribution.

Expansion value depends on additional merchants, agents, rails, geographies or autonomous use cases. It should be probability-weighted using integration, certification, regulatory, customer and control evidence. Strategic optionality can remain outside the base price or enter contingent consideration.

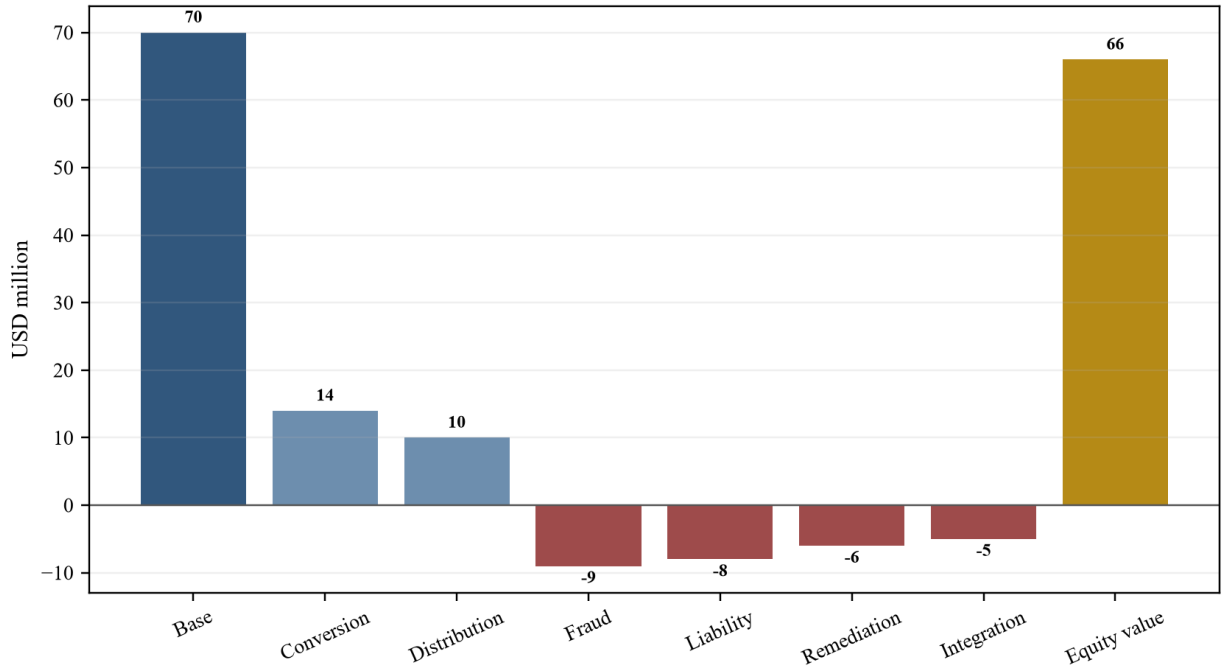
The hypothetical valuation begins with USD 70 million of stand-alone value. It adds USD 14 million for evidenced merchant-conversion improvement and USD 10 million for buyer distribution. It deducts USD 9 million for immature fraud cohorts, USD 8 million for liability uncertainty, USD 6 million for technology remediation and USD 5 million for integration. The resulting illustrative equity value is USD 66 million. Every amount is a management assumption and not a valuation opinion.

**Table 6. Hypothetical evidence-layer valuation**

| Layer | Gross value | Evidence weight | Included value |
|---|---|---|---|
| stand-alone operating value | 70 | 100% | 70 |
| merchant conversion | 14 | 100% | 14 |
| buyer distribution | 20 | 50% | 10 |
| immature fraud cohorts | (9) | 100% | (9) |
| liability uncertainty | (8) | 100% | (8) |
| technology remediation | (6) | 100% | (6) |
| integration | (5) | 100% | (5) |
| illustrative equity value | | | 66 |

*Wholly hypothetical USD millions and evidence weights.*

**Figure 4. Hypothetical equity-value bridge**




*Wholly hypothetical USD millions; the bridge is methodological and is not a valuation opinion.*

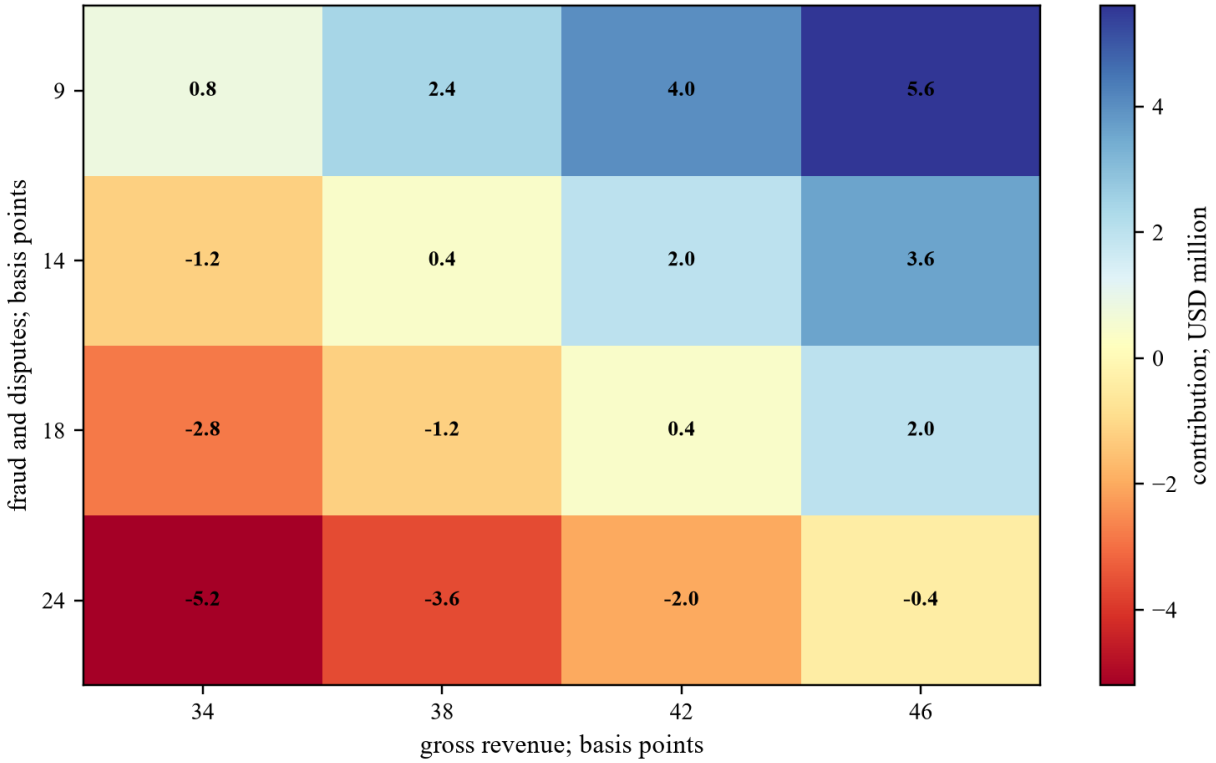
## 19. Apply a liability discount transparently

A liability discount should quantify uncertainty that current authority, fraud and dispute outcomes will not persist after scaling or change of control. It should connect to identified scenarios rather than a generic percentage. Relevant drivers include unseasoned transaction cohorts, ambiguous mandates, unsupported authentication exemptions, merchant concentration, contractual gaps, weak evidence retention and uncertain regulatory perimeter.

The hypothetical central case uses the economics in section 12. The downside assumes fraud and dispute cost rises from 9 to 18 basis points, agent and authentication cost rises from 3 to 5 basis points, and gross revenue falls from 42 to 38 basis points because of pricing pressure. The severe case assumes 24 basis points of fraud and disputes and a temporary 20 per cent reduction in processed value. These are management assumptions, not probabilities.

The board should identify the first date at which contribution, liquidity, a network condition or minimum reserve fails. Management actions need amount, owner, lead time and customer effect. Possible actions include restricting autonomy, increasing authentication, suspending an agent or merchant, changing limits, adding reserves or obtaining indemnity.

**Figure 5. Hypothetical contribution sensitivity**




*Wholly hypothetical annual USD millions across fraud-and-dispute and revenue cases.*

## 20. Translate evidence into transaction protections

The purchase agreement should convert identified uncertainty into allocation, conditions, price and operating commitments. Representations should address licences, scheme status, authority records, data rights, security, fraud metrics, disputes, reserves, merchants, keys, models, vendors and incidents. Definitions should match the diligence data.

Conditions may include network or regulatory consent, key and certificate control, transfer of critical contracts, remediation of a material authority gap, reserve funding and delivery of reproducible evidence. Covenants should govern material model, policy, credential and vendor changes between signing and closing.

Indemnities, escrow, retention and insurance should match enforceable exposure. Deferred consideration can depend on seasoned fraud cohorts, merchant retention, dispute outcomes and verified contribution. The buyer should avoid milestones based solely on gross payment value or agent traffic.

**Table 7. Evidence-to-protection matrix**

| Evidence gap | Price response | Protection | Release evidence |
|---|---|---|---|
| unseasoned fraud cohort | value deferral | retention or earn-out | mature net loss and contribution |
| ambiguous authority | remediation deduction | condition and indemnity | verified mandate and dispute test |
| network approval pending | contingent expansion value | consent condition | written approval and production test |
| non-transferable data right | exclude dependent value | representation and covenant | executed transferable right |
| weak evidence retention | funded remediation | escrow and milestone | reproducible historic sample |

| Evidence gap | Price response | Protection | Release evidence |
|---|---|---|---|
| vendor concentration | continuity deduction | transition covenant | tested alternative and exit |
| known incident exposure | specific deduction | indemnity and reserve | closure and quantified residual risk |

*Proposed framework; qualified advisers should draft enforceable terms.*

## 21. Design integration around payment continuity

Integration can change agents, keys, credentials, policies, merchants, processors, data and customer communication at once. Day One should preserve legal entities, licences, scheme status, payment routing, settlement, reserves, dispute deadlines, fraud monitoring, revocation and incident response.

Control ownership should be explicit. The buyer should establish one decision record for material changes to authority, authentication, credentials, fraud rules and models. Parallel operation may be appropriate where a failure could create duplicate payment, customer harm or scheme breach.

Merchant and network communication requires sequencing. Rebranding, domain changes, certificate rotation, processor migration and contract novation can alter trust signals. The integration plan should identify which changes require approval, re-certification, customer notice or renewed consent.

Synergy should follow continuity. Distribution, cross-selling and shared infrastructure can create value after authority, fraud, evidence and settlement remain stable under the combined operating model.

## 22. Execute a 180-day programme

The first thirty days should establish control. Confirm cash, settlement, reserves, licences, network status, merchant contracts, agent registrations, keys, model inventory, fraud queues, disputes, incidents and critical vendors. Freeze undocumented changes and preserve transaction evidence.

Days thirty-one to ninety should reproduce sampled transactions, test mandates, reconcile fraud and disputes, validate unit economics, exercise revocation, test idempotency and complete role-specific legal analysis. Material gaps should enter funded remediation plans with owners and deadlines.

Days ninety-one to one hundred and eighty should complete approved integrations, obtain consents, rotate keys where required, automate evidence, close high-priority findings, season transaction cohorts and release value initiatives that meet their gates. The board should see customer, control, cash and liability outcomes together.

### Transaction reconstruction protocol

The team should select samples across agents, merchants, rails, geographies, authentication paths, successful payments, declines, refunds and disputes. For each item, it should reconstruct user instruction, consent surface, mandate, checkout, credential, authorisation, fulfilment, settlement and cash. Stable identifiers and event times should connect every record.

Reconstruction should use immutable source extracts with documented lineage, control totals and duplicate treatment. The team should compare the transaction presented to the user with the transaction executed. Any inability to reproduce scope, amount, merchant or instrument should be classified by root cause and potential liability.

### Authority and revocation protocol

The team should test specific and open mandates, spend caps, merchant restrictions, time windows, recurring authority, instrument limits and exception approval. It should attempt reuse outside scope and confirm deterministic rejection.

Revocation tests should cover the user, agent, credential, device and merchant. The board should see propagation time across caches, providers and networks. A technically valid revocation that arrives after execution may still leave financial and customer exposure.

## Fraud and dispute protocol

Fraud cohorts should reconcile attempts, blocks, authorisations, losses, recoveries and final classification. Disputes should reconcile reason, evidence, deadline, provisional credit, result and cash. The same definitions should appear in operational dashboards, contracts and valuation.

The team should replay closed disputes and assess evidence completeness without relying on the employees who originally handled them. It should estimate the cost and loss effect of missing records, unsupported classifications and immature cohorts.

## Economics and liability protocol

Contribution should be rebuilt by rail, agent, merchant and cohort. Revenue should reconcile to settlement and bank receipt. Processing, network, authentication, fraud, disputes, incentives, support, compliance and partner shares should be visible.

Legal analysis should map each material failure to applicable law, scheme rule and contract. The operating model should carry the same allocation. A loss attributed to a merchant in the forecast cannot remain an unreserved platform obligation in the legal review.

## Scenario governance protocol

The model should distinguish external conditions from management choices. Attack rates, merchant behaviour, network rules and regulatory change may be external. Agent limits, authentication, pricing, reserves, product scope and vendor configuration remain partly controllable.

Reverse stress testing should identify the combination that causes negative contribution, reserve shortfall, network breach, licence concern or unacceptable customer outcome. The output should guide price, retention, indemnity, reserve funding and integration sequence.

## Merchant and network acceptance protocol

The team should distinguish protocol compatibility from commercial acceptance. For each material merchant, acquirer, network and credential provider, it should record the production status, technical certification, contract, volume limit, supported geography, payment method, dispute process and change-of-control requirement. Announced participation, sandbox connectivity and a signed pilot should remain separate from accepted production volume.

Merchant testing should compare agent-recognised and conventional traffic across availability, checkout completion, authentication, authorisation, fulfilment, cancellation, refund and dispute. The analysis should identify where merchants continue to classify legitimate agents as bots and where agent-specific paths weaken ordinary fraud or inventory controls. Control changes should have named owners and rollback criteria.

Network and processor evidence should confirm how agent indicators, tokens, mandates and authentication results enter authorisation and dispute messages. The team should identify fields that are lost between systems or reduced to proprietary logs. A valuable control should produce evidence that reaches the participant responsible for the decision and remains available during a dispute.

## Key, credential and software-supply protocol

The team should inventory signing keys, encryption keys, certificates, token services, credential vaults, software packages, model endpoints and privileged tools. Each item should have an owner, environment,

access rule, rotation schedule, revocation process, dependency map and incident history. Production keys should remain separated from development and testing.

Change-of-control planning should address legal ownership and operational custody. Keys may need rotation, certificates may need reissuance, and network registrations may require approval. The buyer should avoid simultaneous migration of identity, policy, credentials and processing unless evidence shows that rollback and reconciliation remain reliable.

Software-supply tests should cover signed releases, dependency provenance, vulnerability management, build access, secrets scanning and emergency patching. A compromised agent tool or package can alter instructions before conventional payment controls see the request. The control environment should detect unauthorised changes and connect them to affected transactions.

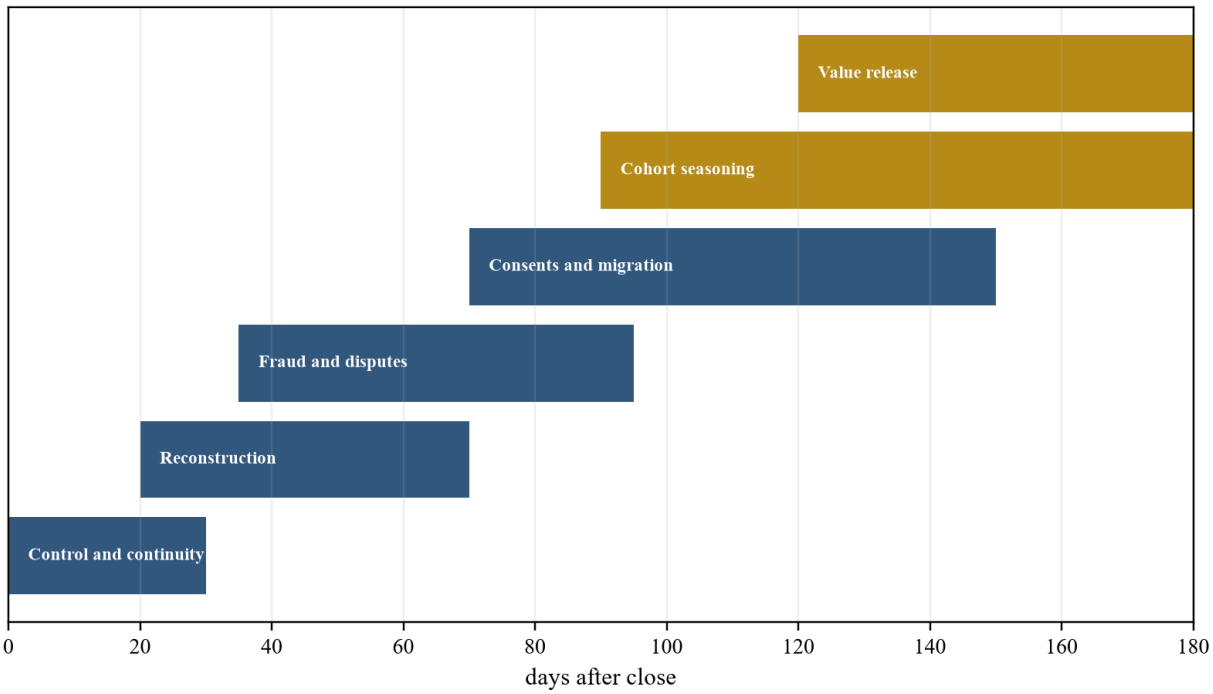
## Ongoing ownership protocol

The combined business should assign one accountable executive for the end-to-end agentic-payment control system, supported by named owners for product, payments, fraud, security, data, legal, compliance, finance and customer operations. Committees should not obscure individual decision rights.

Board reporting should connect agent adoption, recognised traffic, mandate success, authentication, conversion, fraud, disputes, customer outcomes, reserves, contribution and incidents. Metrics should use stable definitions and reconcile to source systems and cash. Material model or policy changes should include expected benefit, control effect, approval, monitoring and rollback.

The operating model should define when an agent, merchant, credential, payment method or geography is restricted or suspended. Thresholds need consequence-based escalation and timely action. Lessons from disputes and incidents should update product design, controls, transaction protections and valuation assumptions for future acquisitions.

**Figure 6. Proposed evidence-gated 180-day programme**




*Timing should follow transaction, network, regulatory and customer constraints.*

## 23. Decision and conclusion

An agentic-payment platform deserves value for a repeatable evidence system that turns delegated intent into authorised, accepted and collected transactions. Agent identity, mandates, tokenisation, authentication and fraud models support that system. Their economic value depends on deterministic enforcement, dispute-grade records, bounded liability, merchant acceptance and stable contribution.

The buyer should reconstruct transactions through time, map every participant and legal role, test authority boundaries, measure conversion and loss together, and reconcile operational labels to cash and liability. Emerging protocols can improve interoperability and evidence, while their adoption and legal effect must be verified in the target's actual products and jurisdictions.

The liability discount should quantify unseasoned cohorts, uncertain authority, contractual gaps, unsupported exemptions, evidence weakness and integration risk. Transaction terms can retain contingent value through milestones tied to mature loss, verified contribution, consent and control evidence.

The resulting acquisition decision is practical. A premium is supportable when the target has transferable registrations and rights, reproducible authority, scoped credentials, effective fraud control, dispute evidence, compliant customer outcomes and collected economics. Price protection, narrower scope, remediation, reserve funding or delayed value is appropriate when those conditions remain incomplete.

## Frequently asked questions

Q: What is the main valuation unit for an agentic-payment platform? A: A transaction whose user authority, agent identity, checkout, credential, authorisation, fulfilment, settlement and collected economics can be reconstructed under one consistent evidence standard.

Q: Does a trusted-agent certificate prove that the user authorised a purchase? A: No. Agent recognition proves facts about the software participant and trust framework. User identity, instruction, mandate, checkout approval and credential scope require separate evidence.

Q: Why are mandates important in payments M&A? A: Mandates can bind delegated authority to limits, merchants, time windows, instruments and specific checkouts. They also create evidence for control testing and disputes when their signatures, keys, schemas and receipts remain reproducible.

Q: How should fraud affect valuation? A: Fraud should be measured by transaction cohort and reconciled from attempts through blocks, authorisations, losses, recoveries, disputes and cash. Immature cohorts and weak classifications should reduce forecast confidence.

Q: Who bears liability when an agent exceeds authority? A: The answer depends on the payment rail, facts, law, scheme rules and contracts. The transaction team should map actual authority, authentication, participant roles and enforceable allocation for each product and jurisdiction.

Q: Can gross payment value support a valuation multiple by itself? A: Gross payment value omits take rate, processing, network cost, fraud, disputes, incentives, support, compliance and partner shares. Valuation should use settled and collected contribution with mature loss cohorts.

Q: Which transaction protections address uncertain agentic-payment risk? A: Conditions, representations, indemnities, escrow, reserves, retention and contingent consideration can be linked to consents, mature fraud cohorts, reproducible authority, merchant retention and verified contribution.

Q: What should happen during the first 180 days? A: The buyer should preserve payment continuity, reconstruct authority and cash, test mandates and revocation, reconcile fraud and disputes, obtain consents, close critical control gaps, season cohorts and release value only after evidence gates pass.

# References


**[1]** Google Agentic Commerce, Agent Payments Protocol specification https://github.com/google-agentic-commerce/AP2/blob/main/docs/ap2/specification.md

**[2]** Google Agentic Commerce, Agent Payments Protocol documentation https://github.com/google-agentic-commerce/AP2/blob/main/docs/index.md

**[3]** Mastercard, Mastercard Agent Pay https://www.mastercard.com/us/en/business/artificial-intelligence/mastercard-agent-pay.html

**[4]** Mastercard, Agentic token framework https://www.mastercard.com/us/en/news-and-trends/stories/2025/agentic-commerce-framework.html

**[5]** Visa, Trusted Agent Protocol specifications https://developer.visa.com/capabilities/trusted-agent-protocol/trusted-agent-protocol-specifications

**[6]** Visa, Trusted Agent Protocol getting started https://developer.visa.com/capabilities/trusted-agent-protocol/docs

**[7]** Internet Engineering Task Force, RFC 9421 HTTP Message Signatures https://www.rfc-editor.org/rfc/rfc9421.html

**[8]** FIDO Alliance, FIDO Alliance specifications https://fidoalliance.org/specifications/

**[9]** EMVCo, EMV Payment Tokenisation https://www.emvco.com/emv-technologies/payment-tokenisation/

**[10]** EMVCo, EMV 3-D Secure https://www.emvco.com/emv-technologies/3d-secure/

**[11]** European Banking Authority, Joint EBA ECB report on payment fraud https://www.eba.europa.eu/publications-and-media/press-releases/joint-eba-ecb-report-payment-fraud-strong-authentication-remains-effective-fraudsters-are-adapting

**[12]** Consumer Financial Protection Bureau, Regulation E https://www.consumerfinance.gov/rules-policy/regulations/1005/

**[13]** Consumer Financial Protection Bureau, Liability for unauthorised transfers https://www.consumerfinance.gov/rules-policy/regulations/1005/6/

**[14]** Consumer Financial Protection Bureau, Electronic Fund Transfers FAQs https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/

**[15]** European Commission, Payment services https://finance.ec.europa.eu/consumer-finance-and-payments/payment-services/payment-services_en

**[16]** European Banking Authority, Payment services and electronic money https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money

**[17]** Financial Conduct Authority, Payment Services Regulations https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations

**[18]** Payment Systems Regulator, APP scams reimbursement https://www.psr.org.uk/our-work/app-scams/

**[19]** Central Bank of the UAE, Retail Payment Services and Card Schemes Regulation https://www.centralbank.ae/en/our-operations/payments-and-settlements/regulations/

**[20]** Monetary Authority of Singapore, Payment Services Act https://www.mas.gov.sg/regulation/acts/payment-services-act

**[21]** Financial Action Task Force, Digital identity guidance https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

**[22]** Financial Crimes Enforcement Network, Anti-money laundering regulations https://www.fincen.gov/resources/statutes-regulations

**[23]** Office of Foreign Assets Control, Sanctions compliance guidance https://ofac.treasury.gov/compliance

**[24]** Basel Committee on Banking Supervision, Principles for operational resilience https://www.bis.org/bcbs/publ/d516.htm

**[25]** Basel Committee on Banking Supervision, Principles for third-party risk https://www.bis.org/bcbs/publ/d605.htm

**[26]** National Institute of Standards and Technology, AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework

**[27]** National Institute of Standards and Technology, Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework

**[28]** PCI Security Standards Council, PCI DSS https://www.pcisecuritystandards.org/standards/pci-dss/

**[29]** PCI Security Standards Council, Tokenisation guidance https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

**[30]** International Organization for Standardization, ISO 20022 https://www.iso20022.org/

**[31]** International Organization for Standardization, ISO IEC 42001 https://www.iso.org/standard/81230.html

**[32]** OpenID Foundation, Identity management for agentic AI https://openid.net/wp-content/uploads/2025/10/Identity-Management-for-Agentic-AI.pdf

**[33]** OpenID Foundation, AuthZEN Authorization API https://openid.net/wg/authzen/specifications/

**[34]** World Wide Web Consortium, Verifiable Credentials Data Model https://www.w3.org/TR/vc-data-model-2.0/

**[35]** World Wide Web Consortium, Web Authentication https://www.w3.org/TR/webauthn-3/

**[36]** European Union, Artificial Intelligence Act https://eur-lex.europa.eu/eli/reg/2024/1689/oj

**[37]** European Data Protection Board, Automated decision-making and profiling guidance https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-automated-individual-decision-making-and_en

**[38]** UK Information Commissioner's Office, AI and data protection guidance https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

**[39]** Federal Trade Commission, Safeguards Rule https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

**[40]** Bank for International Settlements, Regulating AI in the financial sector https://www.bis.org/fsi/publ/insights63.htm

**[41]** Financial Stability Board, Artificial intelligence and financial stability https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

**[42]** Board of Governors of the Federal Reserve System, SR 11-7 model risk management https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

**[43]** Bank of England, Model risk management principles for banks https://www.bankofengland.co.uk/prudential-regulation/publication/2023/may/model-risk-management-principles-for-banks-supervisory-statement

**[44]** Financial Conduct Authority, Consumer Duty https://www.fca.org.uk/firms/consumer-duty

**[45]** Consumer Financial Protection Bureau, Personal financial data rights rule https://www.consumerfinance.gov/1033-rule/

**[46]** European Central Bank, Cyber resilience oversight expectations https://www.ecb.europa.eu/paym/pol/shared/pdf/2018/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

**[47]** Committee on Payments and Market Infrastructures, Reducing the risk of wholesale payments fraud https://www.bis.org/cpmi/publ/d178.htm

**[48]** International Valuation Standards Council, International Valuation Standards https://ivsc.org/standards/

**[49]** International Financial Reporting Standards Foundation, IFRS 3 Business Combinations https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

**[50]** International Financial Reporting Standards Foundation, IAS 38 Intangible Assets https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

## About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.