

Merchant Perspectives on E-commerce for Humans and AI Agents

9 September 2026

Merchant Perspectives on E-commerce for Humans and AI Agents



Steve Cole

Director of Technology Engagement



Merchant Perspectives on E-commerce for Humans and AI Agents

Commerce is moving from direct consumer transactions to transactions initiated, negotiated, and executed by autonomous agents on a consumer's behalf. This is a structural change to payments and money movement across the supply chain, not a new consumer interface layered on top.

Agentic commerce challenges the assumptions of the human-in-the-loop model across every stage of the transaction lifecycle. The changes that will result reach well beyond the checkout interface and into much of the existing payments architecture.

The positions set out in this presentation describe the conditions under which merchants can participate in the system on a sound footing. Without these conditions in place, merchants will be exposed to risks they did not cause and have limited ability to identify or manage.

Authorization, Consent, and Liability Allocation

Card-not-present (CNP) rules generally assume that a human buyer made the purchase decision and allocate fraud liability to the merchant by default, unless the transaction is authenticated through EMV® 3-D Secure or an equivalent mechanism.

Agentic commerce complicates that assumption. A transaction may be technically authorized but disputed because an agent exceeded delegated authority, relied on stale instructions, misunderstood the user's intent, or executed outside an approved consent scope.

Existing CNP rules do not address this “authorized-by-agent” scenario, creating a risk that liability defaults to merchants by convention rather than by control over the failure point.

Authorization, Consent, and Liability Allocation

Agentic commerce should adopt a liability waterfall that assigns responsibility to the party controlling the failed function:

- The consumer acting as principal (where the agent acted within authorized scope)
- The agent operator (where the agent exceeded its mandate or malfunctioned)
- The wallet or trust provider (where credential issuance or revocation failed)
- The processor, issuer, or network (where transaction handling or operating rules failed)
- The merchant (where the failure occurred within the merchant's own systems or controls).

A “Human-Not-Present” transaction class is recommended for transactions executed by autonomous or semi-autonomous agents without real-time human confirmation.

Routing Neutrality, Token Portability, and Payment Choice

Existing U.S. debit-routing policy reflects the principle that merchants should be able to choose among eligible networks for covered debit transactions. Agentic commerce creates a new risk that routing control moves upstream.

The key risks are:

- Lock-in risk: If agent-held credentials or mandate-linked tokens are bound to a specific wallet, platform, or processor vault, merchants lose the practical ability to switch processors, negotiate rates, or preserve least-cost routing.
- Upstream routing displacement: When an agent operator, orchestration provider, or wallet selects the credential and payment path before the transaction reaches merchant systems, merchant routing preferences at settlement may be bypassed entirely.
- Regulatory gap: Regulatory precedent in the U.S. established that merchants have enforceable rights over transaction routing. Payment rules have not been updated to include agentic-specific transactions, so there is no clear protection in network operating rules.

Routing Neutrality, Token Portability, and Payment Choice

Two principles should govern routing and token design in agent-mediated commerce:

1. Preserve merchant routing autonomy. Routing authority for agent-initiated transactions should not be displaced by network participation requirements, agent credential architecture, wallet design, or orchestration protocol rules. Merchants should retain the ability to configure routing preferences, including eligible network selection, payment-method prioritization, and access to a payment credential needed to route agent-initiated transactions. This principle should be embedded in network operating rules as an extension of existing routing protections into the agentic commerce context.
2. Establish token portability and migration rights. Payment tokens, agent credentials, and mandate-linked payment artifacts used in agent-mediated transactions should not create processor or network lock-in. Tokens should be portable across processors and compatible with merchant routing preferences. Agent access should not be conditioned on a merchant establishing a specific processor, vault provider, wallet, or network relationship.

Mandatory Evidence Package Standards

Agentic commerce separates the person who initiates the purchase intent from the software that executes the transaction. This creates an evidence gap.

A transaction may be authenticated at Authorization and still be disputed because the agent exceeded its authority, acted on stale instructions, selected the wrong product, or completed a purchase outside the consumer's approved limits.

In those cases, the merchant needs more than a payment token or authorization response. The merchant needs evidence of what the agent was authorized to do, generated at Authorization and preserved through the dispute window.

Mandatory Evidence Package Standards

A complete evidence record should include, at a minimum, four elements:

1. Agent identity: Proof that the transaction came from a legitimate, registered, or verifiable agent.
2. User verification: Confirmation that the agent was acting on behalf of an authenticated consumer.
3. Consumer mandate: The scope of authority granted to the agent, including price, merchant, product, timing, or category limits.
4. Payment credential and authorization record: A valid payment credential tied to the specific authorized action.

Data Sovereignty and AI Training Boundaries

If data governance is not explicit, merchants may face several risks across Intent and Discovery:

- **Training risk:** Merchant catalog, transaction, or behavioral data may be used to improve AI models without specific merchant consent.
- **Competitive intelligence risk:** Aggregated merchant data may be converted into insights that benefit platforms, other merchants, or competing offers.
- **Discovery risk:** Platforms may use behavioral signals to shape which products are recommended, substituted, or bypassed during Discovery.
- **Relationship risk:** The consumer relationship may shift from the merchant's brand, loyalty program, and post-purchase channels to the agent platform.

Data Sovereignty and AI Training Boundaries

Merchant choice should be the default, and participation in agentic commerce should not require merchants to surrender control over their catalog, transaction, customer, or behavioral data generated at Intent, Discovery, or any other lifecycle stage.

Use of merchant data for AI model training, platform intelligence, recommendation optimization, competitive benchmarking, or derivative data products should require explicit, affirmative, and revocable merchant consent.

Merchants should retain the ability to preserve a direct consumer relationship. Agentic commerce architectures should not, by default, suppress merchant branding, loyalty participation, post-purchase communication, or other relationship-building channels.

Agent Identity and Traceability (Know Your Agent - KYA)

Most merchant payment systems were built to process transactions, not to identify whether the purchase decision was made by a human or by an AI agent acting on the consumer's behalf. This agent visibility problem could become a future risk if not addressed.

Merchants may face several risks:

- Operational risk: Merchants may need to support multiple agent identity frameworks across networks, wallets, agent operators, and processors.
- Fraud risk: Malicious agents may be difficult to distinguish from legitimate agent traffic.
- Dispute risk: Merchants may lack a traceable record of which agent acted, who operated it, and whether it was authorized.
- Governance risk: Network or agent operator that controls agent certification may influence which agents can transact, under what conditions, and thru which payment paths.
- Revocation risk: If compromised or unauthorized agent credentials are not revoked in real time, merchants may process transactions that should have been blocked.

Agent Identity and Traceability (Know Your Agent - KYA)

Agentic commerce requires an open KYA standard with cryptographic verification, traceability, real-time revocation, and merchant representation in governance.

Each AI agent authorized to initiate or execute financial transactions should carry a unique, verifiable digital identifier. The identifier should be traceable to a registered operator, associated with the agent's authorization scope, and verifiable by merchants, processors, acquirers, issuers, networks, and trust providers through an open mechanism.

KYA should not be controlled solely by any single network, wallet, agent operator, or trust provider.

KYA should include real-time revocation.

KYA should be prerequisite for trusted agentic commerce.

Pricing Transparency and Anti-Fee Stacking

Agentic commerce introduces the potential for new fees at various stages of the transaction lifecycle. A single agent-initiated purchase may involve:

- A discovery surface
- An agent operator and orchestration provider
- An identity or trust provider
- As well as existing participants (PSP, acquirer, network, issuer, and wallet)

For merchants, the concern is not that new services will carry a cost, but that agentic commerce fees with no or negligible incremental value to the merchant, may be layered onto existing costs, without clear transaction-level disclosure.

Stacked orchestration, identity-verification, and network-gatekeeper fees could push agent-mediated commerce from expensive to uneconomical.

Pricing Transparency and Anti-Fee Stacking

Agentic commerce requires transaction-level pricing transparency before Authorization.

Every agentic commerce-specific fee should be itemized and disclosed to the merchant before the transaction is authorized. This includes platform facilitation fees, orchestration fees, identity or trust-verification charges, tokenization fees, agent-specific network or processing charges, and any interchange or assessment reclassification tied to agentic commerce.

Disclosure should be machine-readable, transaction-level, and available before Authorization. Bundled or aggregate disclosures should not be treated as sufficient where they prevent merchants from understanding the cost of accepting an agent-initiated transaction.

Open Standards and Interoperability

Agentic commerce is developing through multiple protocols, agent operators, wallets, networks, identity frameworks and payment systems, touching different stages of the transaction lifecycle. Without open standards and interoperability, those systems may become proprietary control points.

The merchant risk has three layers:

- Fragmentation risk: Merchants may need to support multiple implementations across agent operators, wallets, networks and PSPs across the lifecycle.
- Concentration risk: Participants that control discovery, ranking, authorization, payment paths at settlement, evidence, and data may become gatekeepers.
- Disintermediation risk: Merchants may lose visibility into customer intent, substitution logic at discovery, recommendation criteria, post-purchase engagement, and transaction context.

Open Standards and Interoperability

Agentic commerce should have open, interoperable standards that are applied across every lifecycle stage, with meaningful merchant representation in governance.

The standards should cover agent identity at authorization, delegated authority, evidence packages, token portability, routing metadata, data permissions at intent and discovery, fee disclosure, revocation and dispute handling.

Agentic commerce should not require merchants to support proprietary implementations.

Merchants should be able to participate in agentic commerce without surrendering control over customer access, payment routing, data rights, or dispute evidence to a proprietary control point.

Thank You!

