



Mar 24, 2026

Categories:

[Agentic Commerce](#)

[Series](#)

[Publications](#)

Authors:

[Nilesh \(Neal\) Patel](#)

AI Agents Are Starting to Act Inside the Transaction, and Commerce Law Is Not Ready

In March 2026, a federal court issued a preliminary injunction in *Amazon.com Services LLC v. Perplexity AI, Inc.*, finding that an AI shopping agent may have violated federal hacking law — even though the user had expressly authorized the agent to act. The court held that user permission does not override a merchant’s express prohibition. The AI agent’s access was “unauthorized” as a matter of law regardless of what the user intended.

That ruling is a preview of the legal architecture problem that [agentic commerce creates](#). Commerce law was built for human actors making conscious decisions. AI agents that browse, negotiate, select, and pay on a user’s behalf break every assumption it rests on — and the law has not caught up.

1. From Recommendation to Execution

Agentic commerce describes what happens when AI moves past recommendations into execution mode — that is, when the agent does not just surface options but selects, negotiates, and completes the transaction on the user’s behalf. This is powered by “computer use” frameworks that allow AI systems to navigate websites, manage accounts, and initiate payment flows as a digital proxy for the user. The market has already moved in this direction: OpenAI launched Instant Checkout in ChatGPT on Stripe infrastructure; Amazon tested “Buy for Me,” an agentic feature that purchases products from third-party brand sites without the customer leaving the Amazon app. These are not proofs of concept. They are production systems, and the legal architecture they operate inside was not designed for them.

Once AI agents begin to act, familiar legal questions move to the center of the transaction. In the coming weeks, this multi-part series on agentic commerce will work through the six fault lines

where the existing legal architecture is cracking.

2. Six Fault Lines of Agentic Commerce

- **Identity and authentication:** If a merchant cannot distinguish a bot from a human, who is actually “buying,” and who bears the legal consequence?
- **Logging and evidence:** How do you prove what happened in a transaction when the “witness” is a black-box AI system?
- **Delegated authority:** What scope of power does a user actually confer when they click “connect your account,” and what happens when that grant conflicts with a merchant’s terms?
- **Assent and contract formation:** Does a “click” by an agent constitute a binding contract for the human principal?
- **Loss allocation:** When an agent buys the wrong product, accepts the wrong terms, or acts outside its authorization, who pays?
- **Infrastructure control:** How are payment networks, platform gatekeepers, and merchant API rules becoming the de facto regulators of this new market—ahead of courts and legislators?

The rest of this article begins that analysis. The immediate pressure point — as the *Perplexity* ruling makes clear — sits at the intersection of identity, authority, and loss allocation.

Authority Is No Longer Implicit

In conventional e-commerce, authority is usually assumed. If a logged-in user clicks “buy,” the merchant treats the act as authorized because the action, the account, and the person are tightly linked. Agentic commerce weakens that link. An AI assistant may act under broad instructions, inferred preferences, spending limits, or delegated permissions.

The *Perplexity* decision makes the authority problem concrete.

The court’s holding rests on a distinction that will define agentic commerce disputes for years: authority is not a single thing. A user

can grant an agent permission to act, and a merchant can simultaneously prohibit that same agent's access — and the merchant's prohibition wins. That creates a direct conflict between user-delegated authority and merchant-controlled access that no existing legal framework cleanly resolves.

One of the earliest design mistakes in agentic commerce will be treating “agent enabled” as a binary state. It is not. Authority in this setting is layered: authority to browse, compare, negotiate, spend, accept terms, renew, or substitute. These distinctions matter because the legal system does not care if a shopping flow felt “smooth.” It cares whether the challenged act can be attributed to a person or entity in a way that supports enforcement, responsibility, and risk allocation.

Assent Will Be Harder to Prove and Easier to Contest

E-commerce law already devotes considerable attention to notice and assent. The standard playbook—present terms, capture a click, and log the event — is complicated by agentic systems. If an agent accepts terms or modifies a cart under generalized instructions, the evidentiary record starts to look thinner and more contestable.

In the *Perplexity* case, Amazon argued it was unable to distinguish the agent's activity from a human user because the agent failed to identify itself (e.g., via a user-agent string). This is not just a UX issue; it reflects a deeper legal tension about who owns the checkout moment, who presents the operative terms, who captures the evidence trail, and who is left defending the transaction later. As products move toward ambient experiences, a company may know its agent followed a sensible path, but that does not mean it can prove the user authorized the specific outcome in a form that survives a dispute.

Loss Allocation Will Drive the First Real Conflicts

The first major legal pressure point in agentic commerce is likely to be a wave of loss events: purchases made in error, unexpected renewals, or agents selecting the wrong product. When these

disputes arise, every participant in the chain will try to move the loss elsewhere.

The *Perplexity* ruling suggests that if a merchant expressly revokes an agent's access, the agent's creator — and potentially the user — could face not just civil disputes, but potential criminal liability under hacking statutes. This is why agentic commerce should be understood as a risk-allocation problem as much as an innovation story. If card networks and payment processors decide that certain forms of delegated purchasing are too risky or difficult to dispute fairly, they may end up shaping the market before courts or regulators do.

Checkout, Disclosure, and Logging as Legal Infrastructure

In traditional online commerce, lawyers often enter the picture after the interface has largely been set. In agentic commerce, that sequence is likely to fail. A substantial share of the legal outcome will be determined upstream by the initial product design, particularly as it relates to the following protocols:

- **Delegation presentation:** How is the authority to act presented to the user?
- **Constraint controls:** Can the user set spending limits, merchant preferences, or approval rules?
- **Logging detail:** Are logs detailed enough to reconstruct what the agent saw and why it acted?
- **Identification:** Does the agent identify itself to the merchant to ensure “authorized” access and avoid hacking claims?

These design decisions are not merely supportive of legal analysis; they are the legal analysis in operational form.

3. What Companies Should Do Now

Companies building or enabling agentic commerce do not need to wait for AI-specific legislation to identify the pressure points. The immediate task is clear and can be distilled as follows:

- **Define authority with precision:** Separate search authority from purchase, payment, substitution, and renewal authority. Recognize that user permission may not override a merchant's express prohibition.
- **Review transaction flows with dispute posture in mind:** Ensure you can reconstruct what triggered an execution. Implement agent identification to mitigate risks under the Computer Fraud and Abuse Act (CFAA).
- **Revisit terms and counterparty assumptions:** Identify where existing documents are silent or tied to outdated models of authorization.
- **Examine the payments layer early:** Ensure credentials are used in a way that reflects the user's actual authorization.
- **Bring cross-functional teams together:** Legal, product, payments, and trust-and-safety teams must work from the same factual assumptions about how the product behaves.

Before we can argue about what an agent was authorized to do, we have to solve for whether the system knows who is acting at all. That very issue will be the focal point in the next installment of our series on agentic commerce.

For now, the takeaway is this: Agentic commerce changes who appears to act in the transaction, how assent is formed, and how losses are allocated. The companies best positioned for this shift will not treat legal review as a sign-off step, but as a core feature of the product itself. The legal work does not start at the edge of the system; it starts at the center of the transaction.

At FBT Gibbons, we understand the transformative nature of AI and are committed to helping clients comply as they innovate, providing tailored solutions to the AI challenges unique to their industry and business operations. For more information, contact the author or any attorney with the firm's [Data, Digital Assets & Technology](#) practice group.

This article was prepared with the assistance of generative AI tools. The analysis, conclusions, and legal positions are the author's.

Agentic Commerce Series

- [Part 1 — AI Agents Are Starting to Act Inside the Transaction, and Commerce Law Is Not Ready](#)
- [Part 2 — The Identity Problem: Authentication, Fraud, and Who's Actually Buying](#)
- [Part 3 — The Authority Problem: When Does an Authorized Agent Become an Unauthorized Buyer?](#)
- [Part 4 — Contracting by Agent: When the Agent Clicks, Who Assents?](#)
- [Part 5 — When the AI Purchase Goes Wrong, Who Pays, and Who Can Prove It?](#)
- [Part 6 — The Gatekeepers of Agentic Commerce](#)
- [Part 6 \(A\) — The Payment Infrastructure Layer: How Network Rules Already Govern Agentic Commerce](#)
- [Part 7 — Agentic Commerce, Price Control, and the New Antitrust Questions](#)
- [Part 8 — What Epic Reveals About Agentic Commerce](#)

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.