FEBRUARY 11, 2026 • 8 MIN READ

Five questions in-house counsel should ask about agentic commerce

AUTHORS

 Lauren Nickerson

 Rosalie Jetté

 Molly Reynolds

 Mavra Choudhry

 Nic Wall

This is the second article in our series on agentic AI for in-house counsel.

Agentic AI—artificial intelligence systems capable of autonomously planning and performing tasks, making decisions, and interacting with various systems to accomplish specific, pre-defined goals—is gaining recognition as the next evolution of artificial intelligence. Agentic commerce applies this capability to shopping and purchasing, empowering AI agents to coordinate and often fully execute transactions with online retailers: consider, for example, an AI assistant that monitors the price of flights and automatically books tickets once they drop below a certain amount.

To enable agentic AI at scale, companies are developing and adopting open-source protocols that establish a common language between consumer tools, business platforms and payment providers. For instance, in January 2026, Google released its Universal Commerce Protocol (UCP), which was developed in collaboration with several industry partners and is now endorsed by over 20 global partners, including payment networks, payment processors and major retailers. The UCP integrates with Google's Agent Payments Protocol (AP2), which was released last fall. This follows OpenAI's earlier Agentic Commerce Protocol, which enables ChatGPT users to buy directly from certain online sellers without leaving their chat.

As these industry standards move toward implementation and organizations weigh adoption, we share five key questions that in-house counsel of all organizations implicated in agentic transactions—including merchants, networks, payment issuers, agent users and agent providers—should consider.

1. How will consent for AI-initiated transactions be obtained and evidenced?
2. What data is involved in agentic commerce and how is privacy consent obtained?
3. What limits do laws, regulations or best practices impose on agentic commerce?
4. Who is liable for AI agent errors, fraud and other disputed transactions?
5. What internal policy/procedure updates are needed for agentic commerce?

As an initial consideration, in-house counsel should have a firm grasp as to what aspects of agentic commerce their organization is seeking to introduce. Agentic commerce can refer to a number of different functionalities. For example, the UCP has been designed to be modular, allowing businesses to select which capabilities (e.g., check-out, order and identity-linking capabilities) or capability extensions (e.g., discounts) to incorporate. Understanding the scope of the given initiative will be critical to answering the key questions below and advising on applicable risks.

1. How will consent for AI-initiated transactions be obtained and evidenced?

When looking at initiatives related to agentic commerce, in-house counsel should consider how consent will be obtained and proven for transactions initiated and/or completed by AI agents—and whether additional requirements should be imposed on the merchant or payment provider to minimize the risk of a buyer disputing the transaction.

Under current agentic commerce models, some transactions can be preauthorized by users, allowing agents to purchase fully on their behalf. Other transactions may, however, require real-time user consent either because (a) the user did not preauthorize the agent to act on its behalf, or (b) there are regulatory constraints, merchant policies or other factors that require escalation to the user for additional information or express confirmation.

For example, the UCP requires cryptographic proof of user consent for each transaction. When a checkout session is created, the merchant embeds a cryptographic mandate documenting the transaction terms (e.g., price and line items). When the purchase is confirmed, the cryptographic mandate is signed using a key produced by either the AI assistant or the user's digital wallet credentials.

2. What data is involved in agentic commerce and how is privacy consent obtained?

Agentic commerce processes necessarily require the collection, use, disclosure and retention of information—likely including consumers' personal information. Beyond transaction essentials (e.g., payment verification information, session/device/browser information), certain tools may also process information for data analytics, marketing and data sales. These additional purposes may trigger various privacy protections, such as express consent requirements and opt-out rights.

In-house counsel should consider what data is being collected, shared and retained through these systems and ask whether it raises privacy concerns. Current protocols, including the UCP, explicitly recommend legal consultation on privacy and consent issues. Key considerations include:

- **Consent is declarative: the protocol communicates consent but does not enforce it.** Merchants and/or e-commerce platforms are still responsible for actioning users' consent choices and ensuring compliance with privacy obligations.
- **Consent states should align with actual user choices, not the platform default.** Platforms should not assume consent without explicit user action. Where a transaction is fully automated, platforms may need to default consent choices to the least permissive option (e.g., not requiring opt-out for data analytics). This could reduce the efficiency of certain business models that require the collection and processing of data for secondary purposes.
- **Default behavior when consent is not provided is business-specific.** The protocol does not impose any standard response where consent is not provided: businesses must decide their own course of action, taking into account relevant regional privacy laws.

It remains to be seen how organizations will be able to obtain valid and demonstrable consent for fully autonomous purchases, particularly given the notice requirements under Canadian privacy laws.

3. What limits do laws, regulations or best practices impose on agentic commerce?

Depending on the transaction, agentic commerce may engage a range of legal and regulatory requirements, including:

- **Consumer protection laws** that limit the circumstances in which fully autonomous purchases can be made (for instance, considering whether a contract for ongoing performance of obligations could be executed through agentic commerce), and require appropriate age-gating and additional protections for minors.
- **Privacy laws** that require consideration of whether data subjects can provide effective consent to data collection and use when relying on an agent.
- **Product-specific regulations**, such as restrictions on the agentic purchase or sale of regulated goods (e.g., alcohol, cannabis products), or on the import or export of certain products.
- **Anti-money laundering and "know your client" requirements** that require identity verification of a purchaser.

4. Who is liable for AI agent errors, fraud and other disputed transactions?

Another important consideration is how responsibility is allocated when an AI agent initiates a transaction that is later disputed as erroneous, fraudulent or otherwise unintended. In-house counsel should consider:

- **Whether consumer terms contemplate AI-initiated transactions.** Existing consumer terms likely presuppose that transactions are initiated by human users. Consider whether additional terms should be included to address liability for AI-initiated transactions.
- **How to handle unauthorized vs. unintended transactions.** Transactions may be disputed for different reasons, necessitating different responses. For example, organizations may draw a distinction between unauthorized activity (e.g., fraud or rogue agents acting well beyond the scope of their instructions) and unintended activity (e.g., transactions that a human user did not intend, even if they were reasonable based on the instructions/authorizations provided to the AI agent).
- **How responsibility is allocated.** E-commerce already involves a matrix of players responsible for facilitating transactions. Agentic commerce further complicates this matrix. Where fraud or agent error is alleged, how will risk be allocated among these players, including the merchant, network, payment issuer, human user and agent provider? Some risks can be contractually allocated among these players; other aspects may be subject to legislative or regulatory parameters (e.g., consumer protection laws).
- **Whether consumer-level insurance covers the disputed transaction.** Consider whether consumer-level insurance applies in the context of a disputed transaction. For example, if the dispute relates to the purchase of airline tickets, determine whether the consumer has independent trip cancellation insurance or similar insurance through their credit card, and whether that coverage is impacted where the consumer disputes the trip based on an unintended booking on a particular date, or for a particular itinerary.
- **Whether existing dispute resolution mechanisms are sufficient.** Consider what dispute resolution mechanisms are currently in place to address concerns related to e-commerce, and whether they are equipped to resolve concerns related to agentic commerce.

5. What internal policy/procedure updates are needed for agentic commerce?

In-house counsel should review and update:

- **Existing policies/procedures**, including external privacy policies, internal data handling and retention policies, and data subject request processes.
- **Incident response and business continuity plans** to address risks such as agents being hacked or given inaccurate instructions.

- **Risk appetite statements and guidelines**—particularly regarding third-party management where agentic AI is developed or managed by external providers.
- **Insurance coverage**, to account for emerging technological risks.

To discuss these issues, please contact the author(s).