Impact Factor (QJIF): 8.47 E-ISSN: 2583-1615, P-ISSN: 3049-3498

International Journal of Research in Academic World

Received: 12/January/2026 **IJRAW:** 2026; 5(2):192-194 **Accepted:** 19/February/2026

Agentic Commerce is Reshaping E-commerce: What Universal Commerce Protocol (UCP) Changes—and What Merchants Should do Next

[*1]Raghavendar Rao Tadpatri

[*1]Associate Director, Department of Cognizant Moment, Cognizant Technology Solutions, OH, USA.

Abstract

E-commerce is entering a new phase in which AI systems do more than recommend products: they can execute purchasing steps on a shopper's behalf within conversational experiences. This shift, often described as *agentic commerce*, increases the value of convenience and speed, but it also exposes a structural constraint in today's ecosystem: integrations remain fragmented across storefronts, marketplaces, payment providers, identity layers, and assistant surfaces. As a result, each new assistant or commerce surface can trigger repeated one-off connector work for discovery, availability, pricing, promotions, checkout, and post-purchase support. In January 2026, Google and ecosystem partners introduced the Universal Commerce Protocol (UCP), positioning it as an open, interoperable way for merchants and commerce platforms to expose standardized commerce capabilities to compliant AI agents. This manuscript explains what changes when commerce becomes agent-executable rather than purely UI-driven, and why protocol primitives can reduce integration sprawl while improving reliability across conversational and voice-first surfaces. It also provides an implementation-oriented playbook for merchants and platforms, emphasizing staged adoption, explicit customer authorization, end-to-end instrumentation, and trust controls such as approved-vendor enforcement, auditable logs, and transparent substitution and savings behavior. Finally, it outlines key risks and non-negotiables—including fraud, account takeover, unauthorized actions, privacy exposure, and liability allocation—and proposes practical guardrails required for safe, scalable adoption of agentic checkout.

Keywords: Agentic commerce, e-commerce, conversational commerce, Universal Commerce Protocol, UCP, digital checkout, AI shopping agents, interoperability, accessibility, voice commerce.

Introduction

1. The E-commerce Shift: from "Search and Click" to "Ask and Buy"

Over the last few years, e-commerce has been optimized for speed—faster delivery, smoother checkout, and tighter personalization. The next step is more structural: AI agents embedded in consumer surfaces can complete commerce actions, not just present options. Instead of browsing, filtering, and manually checking out, a shopper can describe intent in natural language and allow an agent to complete steps such as product selection, checkout, and post-purchase actions.

This new model can increase conversion potential, but it also exposes a major bottleneck: integrations are fragmented. Every new assistant or commerce surface can create additional connector work for merchants—product discovery, availability, pricing, cart and checkout, payment authorization, order confirmation, and customer support.

2. What UCP is—and Why it Matters

The Universal Commerce Protocol (UCP) is positioned as an open standard intended to provide a common language for agentic commerce across platforms and systems. The core promise is interoperability: rather than building one-off integrations for each agent or surface, merchants and commerce providers can implement UCP once and become reachable by compliant agents.

Google documentation frames UCP as a way to enable agentic actions on Google AI experiences, beginning with direct buying. UCP has also been described as neutral or vendor-agnostic, while providing a concrete reference implementation that powers buying experiences across conversational surfaces (including AI Mode in Search and Gemini).

The practical impact is that commerce becomes less dependent on UI funnels and more dependent on machine-readable capability, trustworthy execution, and well-defined controls.

3. What Changes in the Ecosystem

i). For Merchants and Commerce Platforms:

UCP pushes merchants to expose commerce functionality as standardized primitives: product lookup, availability, pricing, promotions, checkout, and post-purchase support. In effect, the storefront becomes both a human UX and an agent-consumable system.

This does not eliminate brand control. Done correctly, it can improve it. Agents can be constrained to a merchant's

***Corresponding Author:** Raghavendar Rao Tadpatri

authoritative catalog, policies, and fulfillment rules, while preserving the merchant's ability to define what is eligible for autonomous purchase versus what requires explicit confirmation.

ii). For Payments and Identity Flows

Agentic checkout elevates requirements for authorization clarity (what the customer approved), strong security controls, and auditability. Reference implementations emphasize reducing friction through familiar payment and wallet providers (for example, allowing purchase using stored payment and identity information in wallet experiences).

The long-term implication is that payment providers, risk systems, and identity layers become even more central as guardrails for autonomous execution. Teams should assume that "who authorized what" becomes a first-class artifact, not a back-office concern.

4. High-value Use Cases: Where Bots Actually Save Time

Below are practical scenarios where agentic commerce delivers real value—especially for repeat or high-frequency purchasing.

i). Repeat Purchases (The "Weekly List" Problem)

For routine shopping (groceries, household essentials, supplements), the customer's goal is not discovery—it is reliability. A user should be able to say, "Reorder my usual list," and have an agent compile the cart with the preferred merchant(s), check availability, and prepare checkout.

ii). Availability Checks and Substitutions

Out-of-stock is where shopping time disappears. Agentic flows become powerful when the agent can:

- Check availability in real time, and
- Recommend acceptable alternatives based on explicit user preferences (brand constraints, dietary restrictions, price ceiling), then request confirmation when needed.

iii). Promotions, Coupons, and "Deal Friction"

One of the biggest inefficiencies in e-commerce is that customers must hunt: search for offers, remember coupon codes, and compare promotions across multiple places. In an agentic flow, the agent can apply eligible promotions and reduce the decision burden while still presenting the customer with a transparent summary of what was applied and why.

iv). Price-drop Alerts for Trusted Items

Instead of endlessly browsing, a customer can persist a watch list and ask for notifications when prices drop or when promotions appear. This is not just convenience—it changes shopping from reactive to automated.

Note: A device or surface is still involved (phone, desktop, smart display, etc.). The improvement is that the customer does not need a traditional browsing-and-checkout workflow; the interaction can happen through conversation on supported surfaces.

5. Voice and Smart-display Agents as an Accessibility Multiplier

Agentic commerce becomes significantly more valuable when the interface is not a traditional website or mobile app, but a voice-first or smart-display device. Examples include Alexa-enabled devices (for example, an Echo Show or Echo Dot), video or smart display devices, and other home assistants. These interfaces can reduce friction for two high-need groups:

- **People with Disabilities or Reduced Vision:** voice and guided confirmations can replace visually dense browsing and small-screen checkout flows.
- **People with Busy Lifestyles:** the goal is to offload repetitive tasks (weekly groceries, household reorders) without time-consuming search and comparison.

In a practical setup, a user configures an approved vendor list on their personal device—for example, Kroger, Walmart, Whole Foods, and other preferred merchants. The approved list is important because it turns "shopping anywhere" into "shopping from trusted partners," strengthening both trust and predictability.

Once the approved vendors are configured, an agentic bot can handle a typical order workflow end-to-end:

- **Intent Capture:** "Order my usual groceries for this week" or "Add detergent and paper towels."
- **Inventory and Fulfillment Checks:** verify availability for each item (including store and location context where applicable).
- **Substitutions with Personalization:** if an item is unavailable, recommend alternatives aligned to preferences (brand constraints, dietary restrictions, size, price ceiling, prior purchase patterns), and request confirmation when the substitution is non-trivial.
- **Automatic Savings Application:** apply eligible on-file coupons, promotions, and discounts, and present a clear savings summary.
- **Secure Checkout:** execute payment only after explicit customer authorization (voice confirmation, passcode/ PIN, or device biometrics where supported) and provide a post-purchase receipt and order status.

The core point is that accessibility and convenience are not separate features; they are the same outcome produced by better interaction design plus reliable, standardized commerce capabilities.

6. Implementation Playbook (Practical, Incremental)

A common failure mode is attempting full autonomy on day one. A safer path is staged adoption, with clear control points and measurable outcomes.

i). Step 1: Start with a Narrow Scope

Pick a controlled product set: consumables, replenishment items, or a single category with low return risk. Define constraints early (merchant list, thresholds, substitution rules) and treat the first release as an operational pilot.

ii). Step 2: Make Customer Authorization Explicit

Define rules for when the agent can:

- Purchase without confirmation (small total, trusted items, repeat SKUs), versus
- Require confirmation (large totals, substitutions, new categories, address changes).

iii). Step 3: Instrument Everything

You need logs for:

- What the agent requested,
- What the merchant system returned,
- What the customer approved (and when),
- What actually got purchased,
- Post-purchase outcomes (returns, cancellations, customer

support load).

Instrumentation should support both technical debugging and governance. If a customer disputes an order, you should be able to reconstruct the chain of events without ambiguity.

iv). Step 4: Expand to Promotions and Substitutions

Only after the base flow is stable should you add complexity like stacking discounts or advanced substitution logic. Promotions and substitutions are also where trust can be lost quickly, so transparency must scale with automation.

v). Step 5: Add Watch Lists and Notifications

These features create recurring engagement and demonstrate tangible time savings. They also provide a controlled way to introduce autonomy: the user opts into a product or SKU, and the agent monitors it under explicit conditions.

7. Risks and Non-negotiables: Trust, Security, and Liability

Agentic commerce only works if customers trust the system more than they trust their own manual checking. That trust must be earned through predictable controls and reversible outcomes.

Key risks to address include:

- Unauthorized actions (real or perceived),
- Fraud and account takeover,
- Price manipulation and opaque substitutions,
- Privacy concerns (preference inference, purchase history exposure),
- Dispute handling (what happens when "the bot did it" is the explanation),
- Liability allocation (merchant, platform, agent provider, payment provider).

A practical trust model for home assistants and smart displays includes:

- **Approved-vendor Enforcement:** default purchases only from a user-approved merchant list.
- **Strong Confirmation:** a final review step for totals, substitutions, delivery address, and payment method.
- **Role-based Autonomy:** rules that increase autonomy only after repeated successful orders (for example, allow reorders of the same SKU under a small-dollar threshold).
- **Auditable Logs and Receipts:** every agent action should be traceable, explainable, and reversible when feasible.

UCP can standardize communication, but it does not automatically solve governance. Teams must explicitly design for user control, transparency, and reversible outcomes.

8. How E-commerce will Change Next—and Why UCP Adds Durable Value

As more commerce moves into conversational surfaces, the competitive battleground shifts from "best website" to "best agent-executable experience." This creates three durable pressures on the ecosystem:

- **Interoperability Becomes Table Stakes:** merchants that cannot be accessed by agents risk losing demand, even if their product and pricing are strong.
- **Trust Becomes a Product Feature:** clear authorization, predictable vendor choices, and transparent savings summaries will differentiate winners.
- **Personalization Becomes Operational:** preferences (brands, substitutions, dietary needs, budgets) must be enforced consistently across devices and channels.

UCP adds durable value because it can reduce integration sprawl. If a merchant exposes the right capabilities through a standardized protocol, it becomes easier for multiple agents and devices to interact with that merchant consistently. Over time, that can lower costs for merchants, improve reliability for customers, and accelerate adoption of agentic shopping experiences.

9. Conclusion

E-commerce is moving toward a world where customers delegate routine shopping to AI agents operating inside conversational experiences. UCP is a meaningful step toward interoperability in that world.

For merchants and platforms, the opportunity is not just bot checkout. It is reducing customer effort to near zero while increasing confidence through transparent authorization, reliable fulfillment, and measurable value. The teams that win will adopt incrementally, build strong trust controls, and treat agentic commerce as an operational system—not a UI feature.

Quick Summary

- Agentic commerce shifts shopping from browsing to delegated execution via AI agents.
- UCP aims to standardize how agents and merchants communicate across discovery, availability, promotions, and checkout.
- Voice and smart-display devices can make shopping dramatically easier for people with disabilities and for busy households.
- The highest-value flows combine approved vendors, inventory checks, personalized substitutions, automatic savings, and strong security controls.
- The future of e-commerce will favor merchants that are interoperable, trustworthy, and consistently personalized across channels.

References

1. Google Developers. Universal Commerce Protocol (UCP). https://developers.google.com/
2. Universal Commerce Protocol documentation and specification. https://github.com/