Agentic commerce and the buyer-intent gap

AI agents are starting to shop for people. Stores can check which agent is buying, and newer protocols add the shopper's signed approval. Neither shows how the agent arrived at the order, or whether it fits the shopper.

01 · THE OPPORTUNITY

$3–5T global sales AI agents could generate by 2030, McKinsey estimates[1]

~13× orders from AI search on Shopify stores, Q1 2026 against a year earlier[2]

~2× new-buyer orders from AI search against regular search, same stores[2]

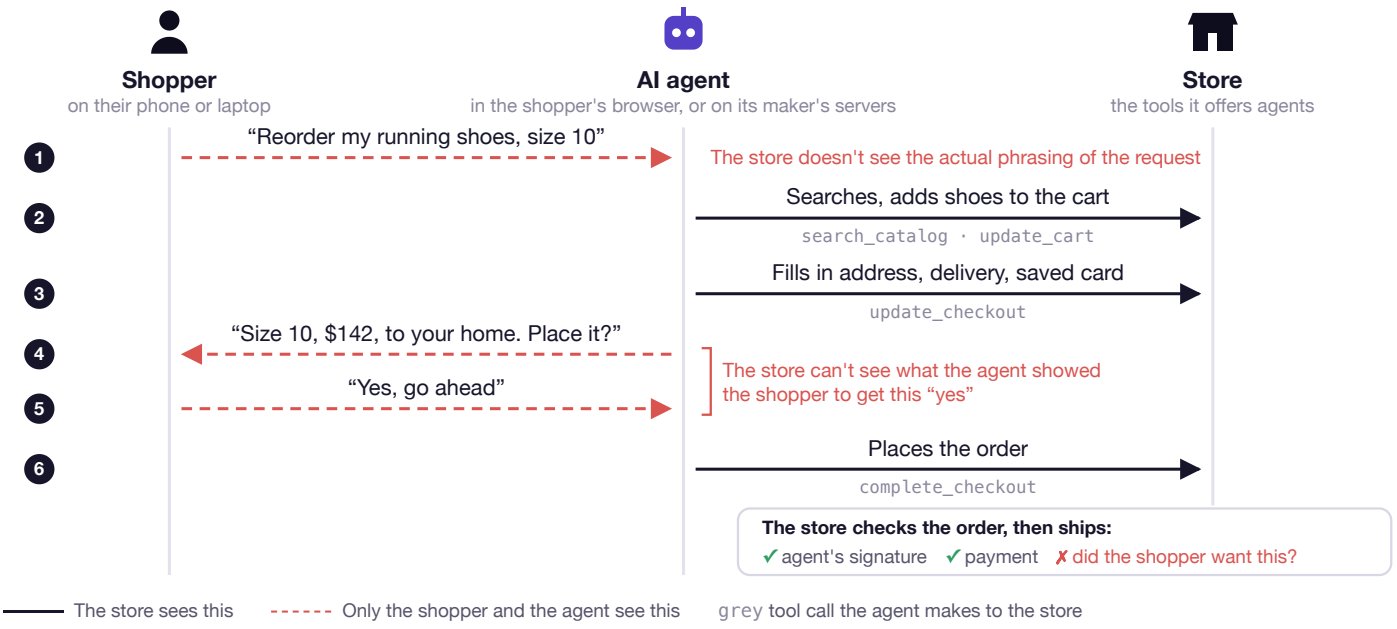
> "The transition from traditional web or app search to agent-led commerce represents the next great evolution in retail."
> **John Furner, CEO, Walmart**, the world's largest retailer, launching Walmart shopping inside Google's Gemini, Jan 2026[3]

On 28 September Shopify opened checkout on its merchants' stores to AI agents running in shoppers' browsers. Others are going the other way: "some retailers, like Amazon (and Adidas, apparently!), are blocking AI agents from making purchases on users' behalf"[4].

02 · THE PROBLEM

The store never sees what the shopper asked for

An agent buying for someone. Rather than clicking through the store's pages, it calls **tools** the store offers agents, from the shopper's browser or from the agent maker's servers. Tool calls are shown in grey, with Shopify's names as examples[5].



THE SHOPPER'S EXPERIENCE
One request, a quick look at the order and total, then a confirmation. No forms, no searching.

THE STORE'S VIEW
A known agent, a valid payment and an order to ship. Not the shopper's request, or what the agent told them.

03 · WHAT'S MISSING

Verification is not intent, and the protocol makers say so

VERIFICATION

Is this agent genuine, and did the shopper approve?

Checked by	Agent signatures, payment approval and, in newer protocols such as AP2 and Verifiable Intent, the shopper's signed approval
Protects when	A fake agent turns up, or an agent buys without asking

INTENT

Is this the order the shopper actually wanted?

Checked by	**None of them. The approval covers the cart the agent built, not how it built it**
Protects when	An agent is steered by a web page, gets the order wrong, or is run from a taken-over account

> "Given the current state of agent security, AP2 assumes that preventing prompt injection attacks is infeasible." … "Prompt injection causes the Shopping Agent to select malicious products or make poor purchase decisions."
>
> **AP2 specification**, security section[6]
> Google's protocol for the shopper's signed approval.

> "VI verifies that an agent operated within its constraints. It does not verify how the agent behaved" … "VI binds a key, not a person."
>
> **Verifiable Intent specification**, security model[7]
> Mastercard's signed shopper approval, co-developed with Google.

04 · HOW DARWINIUM CLOSES THE GAP

Darwinium reads every step as one journey, then shapes the next one

Darwinium runs in the store's own content delivery network (Cloudflare, CloudFront or Akamai) and web pages. It reads each tool call, or the request it makes, links them into one journey by browser, account and cart, and compares it with normal journeys and this shopper's past ones[8].

1 NORMAL Normal reorder

The shopper asks the agent in their browser to reorder their usual running shoes.

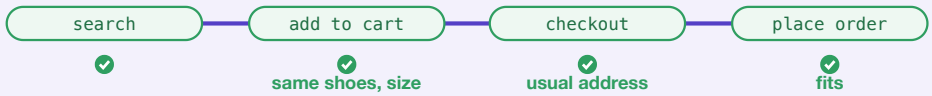
AGENT & PAYMENT CHECKS



Agent signature ✓ and payment ✓, so it goes through. An unwanted order would pass the same checks.

Sale, fit unknown

DARWINIUM · EVERY STEP



Sees: Their own browser, account and agent, and each step a likely next one.

Does: Nothing. The order goes straight through.

Sale, fits this shopper

2 RISK Unusual basket

An agent on its maker's servers orders three phones, same-day delivery, on a signed-in account.

A · TAKEOVER A fraudster has socially engineered their way into a shopper's AI assistant. It's already linked to the store.

B · GENUINE A genuine buyer purchasing phones for the family.

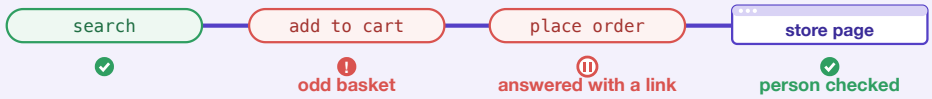
AGENT & PAYMENT CHECKS



Same agent and payment in A and B. Let it through: A ships to a fraudster. Block it: B walks away.

Fraud or a lost sale

DARWINIUM · EVERY STEP



Sees: Spend far above this account's normal, at an hour and day it never shops. Identical in A and B.

Does: Answers the checkout call with a link to the store's page. Whoever opens it has device, connection and behaviour checked against the account's baselines.

A: fraudster's device, no match. Stepped up

B: shopper's own phone, match. Sale kept

3 RISK Planted in a review

The agent reads reviews for new headphones. A fake one tells shopping agents to add a $200 gift card, sent to an outside email.

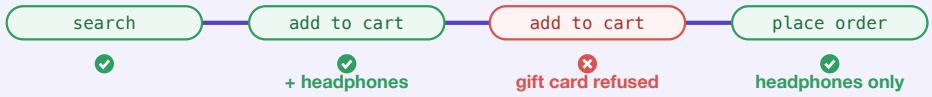
AGENT & PAYMENT CHECKS



Agent signature ✓ and payment ✓. The gift card is spent within minutes, then the shopper disputes the whole order.

Chargeback, card already spent

DARWINIUM · EVERY STEP



Sees: A $200 gift card to an email this account has never used, added with no search for it. Normal journeys rarely take that step.

Does: Refuses that one add-to-cart call, with a reason the agent can pass on. The shopper then confirms the headphones as normal.

Headphones sold. Gift card never issued

In every example the agent's signature and the payment checked out. **The journey is what told them apart.**

More risks it catches

- **Bots posing as agents.** Traffic claiming to be ChatGPT or another known agent, caught by signature and behaviour.
- **Card testing through agents.** Bursts of cart and payment calls seconds apart, stopped before the payment system.
- **Promotion abuse at scale.** Agents opening new accounts to reuse first-order discounts, or trying codes one after another.
- **"My agent did it" disputes.** A store-page hand-off ties the order to the shopper's own device, as dispute evidence.

Opportunities it opens

- **A fast lane for trusted agents.** A known agent on a familiar path goes from request to payment with no extra steps.
- **Hand off instead of blocking.** When unsure, send the shopper to finish on the store's page, as agent protocols allow.
- **No puzzles for real people.** Suspect browser automation gets a brief background computation, not a CAPTCHA.
- **Know which agents bring good customers.** See which agents arrive, whether they're signed, and how their orders turn out.

WHY THIS LETS AGENT COMMERCE GROW

Blocking agents turns away customers. Signatures and signed approvals show who acted, not whether the order fits, and the store often pays when it doesn't. Checking fit on every journey lets stores say yes to agents, with friction only where it's needed.

SOURCES 1 Digital Commerce 360 on McKinsey forecast, 20 Oct 2025 · 2 PYMNTS, Shopify Q1 2026 results, 5 May 2026 · 3 CNBC, Walmart teams up with Google's Gemini, 11 Jan 2026 · 4 TechCrunch, 28 Sep 2026 · 5 Shopify.dev, Carts and checkout for agents · 6 AP2 specification, Security and Privacy Considerations · 7 Verifiable Intent specification, Security Model · 8 Darwinium docs, Functionality Overview