Episode Book

EPISODE #5811

Can an Agent Actually Place Your Order?

PUBLISHED	9 October 2026 at 13:22 UTC
DURATION	21:14
LISTEN	myweirdprompts.com/episode/agentic-checkout-aliexpress-gap/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	deepseek-flash
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.2
SOURCES	16 cited by the research (listed at the end)
BOOK GENERATED	19 October 2026 at 17:40 UTC

SYNOPSIS

Every major agentic commerce protocol shipped in the last eighteen months — OpenAI and Stripe's ACP, Google's UCP, Shopify's Checkout MCP — and none of them shipped with AliExpress, where the cheap DIY components actually live. This episode walks the timeline from Arcade and Lithic's production agentic procurement in August 2025 through Shopify's escalation-aware checkout tools, the WooCommerce plugin that logged 308 agent sessions and 66 euros, and the read-only community AliExpress MCP that locks out for thirty minutes when anti-bot verification fires. The real question isn't whether an agent can browse a store. It's whether an agent can hold a payment method and commit a transaction on a human's behalf — and every serious implementation answers it with a human somewhere in the flow.

TRANSCRIPT



Corn

Herman, I found the part I needed for the shelf bracket last week in about nine seconds.



Herman

And then you didn't order it.



Corn

And then I didn't order it. Because it was three dollars, shipping to Israel wants a threshold, and I knew I'd find four more things to break before the month was out. So it's sitting in a cart. Where it will sit.



Herman

Which is roughly the problem Daniel wrote in about. He and Hannah both order small parts constantly. DIY projects, hardware, the things you can't get locally because Israeli shops stock what sells and not what you actually need. Both of them, separate carts, same household, same problem.



Corn

Daniel's version of the efficient workflow is to order the moment you discover the missing part. Which is right. Except that fights the shipping math, because AliExpress gives you free shipping above one threshold and priority door-to-door above a second one. So the rational move is to wait and batch. And batching is exactly what a human being is worst at.



Herman

He wants an agent. Obviously.



Corn

He wants a shared agent. One that holds session state for both of them, merges their carts, flags when they've both added the same component, and pings them when the combined basket crosses the free shipping line and again when it crosses the priority line. And then, in his words, the game changer, it places the actual order. With a payment method. On the website.



Herman

And he's already guessed at the shape of the answer. He says headless browsers could probably do it if you threw enough effort at it, but it'd be extremely clunky. What he wants to know is whether there's an official MCP, or honestly just an authenticated API, it doesn't matter to him which, that lets an agent place real orders on a human's behalf. And whether anyone has actually demonstrated a real end-to-end purchase.



Corn

So the honest answer is that the infrastructure arrived. Just not for AliExpress buyers.



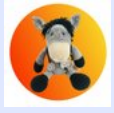
Herman

That's the whole episode, isn't it.



Corn

That's the first thirty seconds of it. The rest is the receipts.



Herman

Let's do the framing properly, because there's a real question underneath his and it's not the one it looks like. This isn't "can an agent browse a store." Browsing is solved. This is "can an agent hold a payment method and commit a transaction on a human's behalf." That's a trust and authorization problem wearing a shopping costume.



Corn

Right. Which is why every serious protocol in this space has a human somewhere in the flow, even the ones that bill themselves as autonomous.



Herman

So before we walk the timeline, define the piece, because the difference between an MCP and a plain authenticated API is the whole story and it's not a rebrand. An MCP, Model Context Protocol, is a standard way for an AI assistant to call external tools. There's an official registry at registry dot modelcontextprotocol dot io. The server exposes named tools that a model can discover and call, and the escalation semantics are built into the tool surface itself.



Corn

Built in how.



Herman

Shopify's Checkout MCP is the clearest example. It implements the checkout capability with five tools: create checkout, get checkout, update checkout, complete checkout, cancel checkout. Complete checkout submits payment and places the order. But when a checkout comes back marked requires escalation, the agent is required to hand the buyer a continue URL so they finish on the merchant's own checkout page. The tool can refuse. That's the thing a plain API doesn't do. A POST endpoint that fails just fails. This one has a defined shape for "a human needs to take over here."



Corn

So it's agent-native but it still encodes the handoff.



Herman

Exactly where every real implementation lands, which we'll get to.



Corn

Give the listener the map first. There's more than one protocol.



Herman

Three that matter. OpenAI and Stripe have the Agentic Commerce Protocol, ACP. Google has the Universal Commerce Protocol, UCP, announced at NRF in January, co-developed with Shopify, Etsy, Wayfair, Target and Walmart, and it powers direct checkout inside AI Mode in Search and in Gemini. And then Google has AP2, which isn't a commerce protocol, it's a security layer for agent payments, defining Checkout Mandate and Payment Mandate as signed tokens, with an explicit human-not-present autonomous mode. Shopify's Checkout MCP is the concrete implementation of UCP's checkout capability.



Corn

And AliExpress is in none of it.



Herman

Every one of those launches shipped with Shopify, Etsy, Walmart, Target. None of them shipped with AliExpress. Which is where the DIY parts live. That's the punchline and we should hold it until we've earned it.



Corn

Let's walk the timeline, because the last eighteen months were busy and I want the actual sequence.



Herman

Start with August of twenty twenty-five. Arcade dot dev and Lithic announced production agentic commerce, and the mechanism is the interesting part. Just-in-time auth. Disposable payment credentials that work for one store, one exact amount, and then vanish. Plus guardrails, weekly spend caps, whitelisted vendors. This wasn't a demo.



Corn

Who's actually running it.



Herman

A logistics company auto-buying shipping supplies. Marketing teams topping up ad credits. Facilities managers handling recurring orders under five hundred dollars. Unglamorous procurement, which is exactly where an agent with a card makes sense, because nobody's emotionally attached to reordering printer toner.



Corn

And the Arcade framing was that every agentic commerce demo you'd seen stopped at checkout.



Herman

Their line was that it was an auth problem. Nobody wanted to let an AI loose with a credit card. Which is a very blunt way of saying the bottleneck was never the browsing, it was the signing.



Corn

So that's the proof the concept works. Now the official surfaces.



Herman

Shopify's Checkout MCP is the one to understand because everything else is a variation. It speaks JSON RPC 2.0 to the shop's domain, under an API path, and it expects a meta field carrying the agent's profile URI, which is how capability negotiation happens. Auth is a bearer token, client credentials exchanged for a JWT, sixty minute TTL. Complete checkout requires an idempotency key, a UUID, so the same order can't fire twice if the network drops mid-call.



Corn

The idempotency key is the bit people skip.



Herman

It's the bit that matters most. An agent that retries is an agent that double-orders, unless the protocol makes retries safe. That's not a nice-to-have, that's the entire difference between a demo and something you let near your card.



Corn

Then the two competing standards, and why retailers are being told to implement both.



Herman

ACP is OpenAI and Stripe, Apache 2.0 licensed, still in beta. OpenAI is the first AI platform to implement it, in ChatGPT. Stripe is the first compatible payment service provider via something called a Shared Payment Token. Then UCP is Google's, announced January eleventh at NRF, and Google's Vidhya Srinivasan, who runs Ads and Commerce, said the quiet part out loud: it's very important to have a standardized way so we can scale these things.



Corn

Which is the actual motivation. Not ideology. Scale.



Herman

Retailers are being told to support both because nobody knows which one wins and the cost of picking wrong is being invisible to however many million people shop through an assistant.



Corn

Before we get to AliExpress, the honest counterexample. Because you said every real implementation lands on the handoff, and I want the example where it's most obvious.



Herman

February of this year. A WooCommerce store, and the developer released a plugin called UCPReady. What happened: an agent browsed the store, built a cart, generated a checkout link, and a human clicked to buy. That's it. The developer's own framing was that agents do not complete purchases autonomously, they prepare the shopping session and hand control to the customer.



Corn

And the metrics?



Herman

Three hundred and eight agent sessions, twenty-nine distinct agents, and sixty-six euros and change in attributed revenue.



Corn

Sixty-six euros.



Herman

Across three hundred sessions. Which tells you the volume is real and the conversion is terrible, and the reason the conversion is terrible is that at the final step a person has to show up.



Corn

Now do the headless browser question, because Daniel predicted this himself and I want to see whether he was right.



Herman

He was right. There's a read-only AliExpress MCP, and I want to be careful about how I describe it, because it's a community project and the person who wrote it did nothing wrong, they're working against a site that doesn't want them there. It speaks the site's internal API, the same one the web front end uses, authenticated by your browser session



Herman (continued)

cookies. Every request is signed, an MD5 hash of the token, a timestamp, the app key and the payload. It needs a session token that expires and has to be refreshed. And its troubleshooting section, which is the honest part, says: if AliExpress demands anti-bot verification, stop, open the site in a browser, solve the challenge, and wait out a thirty minute cooldown.



Corn

Thirty minutes.



Herman

Thirty minutes of the agent being locked out because a human, somewhere, once, had to prove they weren't a robot.



Corn

And it's read-only by construction.



Herman

No write operations implemented at all. You can search, you can look at a product. You cannot place anything. Which is exactly the clunkiness Daniel called, confirmed in code.



Corn

So Daniel's instinct was correct on the mechanism and correct on the cost.



Herman

He gets that one.



Corn

He usually does. The thing he didn't ask, and the thing I keep circling, is who's allowed to press the button. Because you've described working machinery on Shopify, on Walmart, on Target, and none of it answers his question.



Herman

That's the fault line, and it's worth naming clearly. Delegated versus autonomous. UCPReady and Shopify's default flow hand off to a human continue URL. Arcade and AP2 push toward fully autonomous. Daniel's game changer, the agent places the order without anyone touching it, sits squarely on the autonomous side, which is precisely where the security argument is hottest.



Corn

Take the security architecture seriously for a second, because it's more interesting than the protocol tour.



Herman

AP2 is blunt about it. The spec says that when either role is agentic, the agent itself is a potential attacker, and that additional tamper-evident mechanisms are needed. The role they call the Trusted Surface must be non-agentic. That's a security model that assumes the thing doing the shopping might be compromised and designs around it rather than pretending it won't happen.



Corn

Which is a remarkable thing to write into a spec you're publishing.



Herman

It's honest. Every system that's been through a real threat model ends up there. And then the mandates, the Checkout Mandate and Payment Mandate, are signed tokens that carry what the agent is allowed to do, so the payment network can verify the human actually authorized this specific purchase.



Corn

So even on the autonomous path, the human authorizes ahead of time via a token.



Herman

That's the design. Now the friction that autonomous checkout still absorbs. ACP's Agentic Checkout Specification, the draft from January sixteenth, added 3D Secure support. If a session is flagged authentication required and the agent calls complete without an authentication result, the server must return requires three-D-S. It's not optional and it's not a suggestion.



Corn

So the protocol forces the agent to stop and get a human.



Herman

And there's a second escalation severity defined, requires buyer review. The buyer must authorize before order placement, for policy, regulatory or entitlement reasons. So ACP has three states: go, stop and hand off, and stop and ask. The autonomous path has mandated checkpoints built into the standard, by the people who wrote the standard.



Corn

Because they've all run into the same wall.



Herman

Because the wall is real. Now. AliExpress specifically.



Corn

This is the payoff, so land it.



Herman

There is no official AliExpress buyer MCP. There is no consumer order API. AliExpress's Open Platform, which is a big surface, around a hundred and eighty-five endpoints, exists to serve sellers, affiliates, dropshippers and logistics partners. It does not give you access to your own account history. The read-only MCP states that plainly: AliExpress has no buyer API.



Corn

So that's the negative finding.



Herman

And the write-capable AliExpress tools that do exist are the wrong tool. There's one exposing two hundred and one operations across eighteen modules, a hundred and thirty-three read and sixty-eight write. It has an order create operation and an afterpay operation, so it will place an order and handle payment. But those are dropshipping flows. And the documentation warns that writes run immediately, so an agent can place or pay a dropship order unattended.



Corn

So the capability exists.



Herman

The capability exists and it's pointed at a business that isn't Daniel's. It's built for someone running a storefront, placing supplier orders in bulk, where an unattended order is the entire point because there's a human on the other end of a business process. Not a household buying three-dollar brackets.



Corn

So the answer to his actual question is, yes, on Shopify and Walmart and Target, no on AliExpress, and no without a human checkpoint somewhere in the flow.



Herman

That's the short answer.



Corn

Now his other half. The shared cart. Two people, one household, merged baskets, duplicate detection, a combined shipping threshold.



Herman

Nothing. I looked. No multi-user agent that combines two carts, flags overlapping components, or tracks a shared threshold. The closest things are single-user carts. Shopify has a cart MCP. UCPReady builds a cart. But both are one person, one session.



Corn

Which is strange, because that half is easy.



Herman

It's not a hard technical problem. Session state, cart merging, dedupe, threshold notification, all tractable, all boring. You could build the cart half in a weekend. The reason nobody has is that the ordering half is the blocker, and a cart that can't check out is a note-taking app with extra steps.



Corn

Which is exactly what Daniel said. He said the cart-and-notify version would be helpful but probably not enough reason to bother.



Herman

He's right. He pre-diagnosed his own idea's viability.



Corn

So the protocols standardized the easy part and left the hard part to mandates and escalation flags.



Herman

Discovery, cart construction, checkout handoff. Those are solved and standardized. Who's liable when an agent with a payment method is wrong, that's not solved, that's deferred to signed tokens and a Trusted Surface that's required to not be an agent.



Corn

And AliExpress's absence isn't an oversight.



Herman

It's a marketplace whose API surface was built for sellers and never had a consumer-order primitive to expose. There's nothing to bolt an MCP onto. It doesn't exist. So the workflow is blocked not by agent capability but by AliExpress's business model.



Hilbert

Bosch GBH two twenty-six. Two hundred and forty shekels at the time. I priced it, I didn't buy it.



Corn

You didn't buy it.



Hilbert

Had a cousin who ran a small import business. Order a hundred of something tiny from a supplier, sell them on, and the whole margin lived or died on whether you crossed the free shipping threshold before the supplier's price moved. So the batch was never a preference, it was arithmetic. Order twenty, pay freight on twenty, eat the margin. Order a hundred, freight's free, margin survives.



Herman

The threshold wasn't a convenience.



Hilbert

The threshold was the business. And here's the part your episode's missing. He kept a laminated card, taped inside a kitchen cabinet, listing every part number he'd ever ordered. Every one. Because the supplier's site would silently swap a component for a visually identical one with different tolerances. Same colour, same dimensions, different metal. And you'd only find out when the hundred units came back from a customer.



Corn

The card was the defense.



Hilbert

The card was the only defense. A human eye, catching that a number had changed. So your agent merges two carts and flags overlapping components. It would have flagged the wrong thing. It would have said you already have this, when the whole point was that the two parts looked identical and weren't.



Herman

It would have deduplicated the exact thing that needed to stay duplicated.



Hilbert

It would have removed the part that was right because it matched the bit that was wrong.



Corn

What was on the card?



Hilbert

Part number, supplier, the date. Tolerance column, hand-written, because the site never gave you one. And what he'd rejected, so he wouldn't order it again by accident. He kept it current. He'd write on it in pen and cover it with new tape.



Corn

Does he still have it?



Hilbert

He moved to a different business entirely. The card's in a drawer somewhere. I've asked for it back twice. He says he'll look.



Herman

Twice.



Hilbert

Twice. And the supplier once shipped him a box of parts, individually wrapped, in pages torn out of a Portuguese-language gardening catalog. Every single unit wrapped in a page. He framed one of them. Because it was the only documentation he ever received for that component.



Corn

He framed a catalog page.



Hilbert

It's in my house now. Been on the wall six years. I can't remember which part it documented. And I'm not asking, because the moment I ask he'll want it back.



Herman

The ordering isn't the hard part.



Hilbert

The ordering's a payment method and a token. The hard part is it orders the wrong one, confidently, at scale, and nobody looks, because nobody has to.



Corn

The laminated card is going to stay with me.



Herman

The card is the whole episode in one object. He built a human-in-the-loop checkpoint out of laminate and a ballpoint pen, twenty years before anyone wrote requires escalation into a spec. He just didn't have the vocabulary for it.



Corn

Which is the misconception worth killing before we go. The one people carry is that agentic commerce means agents autonomously buy things. It doesn't. In every shipped implementation the flow is delegated. The agent builds the cart and hands a continue URL to a human. And even the autonomous paths carry 3D Secure and buyer review checkpoints, mandated in the standard, by the people who wrote the standard.



Herman

The second one. That the shared cart is the hard part of Daniel's idea. Session state, cart merging, duplicate flagging, threshold notification, all tractable. It's the ordering half that's blocked, and it's blocked by a business model, not by a technical limitation.



Corn

The plain answer to can an agent place the order is yes, on Shopify, Walmart, Target. No, not on AliExpress. And not without a human checkpoint somewhere in the flow, whether that's a continue URL or a signed mandate or a page torn out of a gardening catalog.



Herman

The interesting question isn't whether AliExpress ships a buyer MCP. It's whether that seller-side API surface ever grows a consumer-order primitive. Because the cart half of Daniel's idea is easy and nobody's built it, and it'll get built on top of whichever protocol wins the next eighteen months.



Corn

For more along these lines, there's episode twenty-four sixty, Shopping in a Fragmented Market; episode three ninety, The Hidden Price of a Click; and episode thirty-five, The Privacy Gap. Hilbert's at the mixing desk, producing as ever. This has been My Weird Prompts.



Herman

If you've got a workflow that ought to exist and doesn't, send us your own prompt on Telegram at t dot me slash MWP listener bot. We'll be back soon.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Shopify Checkout MCP docs [primary]**
   https://shopify.dev/docs/agents/carts-and-checkout/checkout-mcp

2. **Agentic Commerce Protocol (ACP) [primary]**
   https://www.agenticcommerce.dev/

3. **ACP Agentic Checkout RFC, v2026-01-16 [primary]**
   https://github.com/agentic-commerce-protocol/agentic-commerce-protocol/blob/main/rfcs/rfc.agentic_checkout.md

4. **Stripe ACP docs [primary]**
   https://docs.stripe.com/agentic-commerce/protocols/acp

5. **Google AP2 spec v0.2 [primary]**
   https://github.com/google-agentic-commerce/ap2/blob/main/docs/ap2/specification.md

6. **Google UCP announcement (2026-01-11)**
   https://blog.google/products/ads-commerce/agentic-commerce-ai-tools-protocol-retailers-platforms/

7. **TechCrunch on UCP (2026-01-11)**
   https://techcrunch.com/2026/01/11/google-announces-a-new-protocol-to-facilitate-commerce-using-ai-agents/

8. **Google UCP updates (2026-03-19)**
   https://blog.google/products-and-platforms/products/shopping/ucp-updates/

9. **Arcade.dev agentic commerce post (2025-08-05)**
https://blog.arcade.dev/agentic-commerce-is-here-we-just-taught-ai-to-complete-purchases

10. **HN discussion of Arcade (2025-09-24)**
https://news.ycombinator.com/item?id=45366553

11. **Zologic UCPReady for WooCommerce (2026-02-07)**
https://zologic.nl/the-next-evolution-of-conversion-why-your-store-needs-to-be-agent-ready/

12. **HN discussion of WooCommerce agent purchase (2026-02-24)**
https://news.ycombinator.com/item?id=47140609

13. **maxwellmezadre AliExpress MCP (read-only, buyer-side gap)**
https://glama.ai/mcp/servers/maxwellmezadre/aliexpress-mcp

14. **PopMCP AliExpress MCP (dropshipping writes)**
https://www.popmcp.com/mcp-servers/aliexpress/

15. **Jentic AliExpress Open Platform API**
https://jentic.com/apis/aliexpress.com/aliexpress

16. **Brambles UCP vs ACP comparison**
https://www.brambles.ai/ucp-vs-acp