The buyer moves to the agent and the loss stays with the seller

5 November 2026 | Strategic Intelligence Division | Ownership

Both agent checkout protocols keep the loss with the seller in their own words. The business remains the Merchant of Record; the merchant remains the system of record for orders, payments, taxes and compliance. The catalogue, the buyer and the price record move to the agent. Returns and exchanges sit outside the draft protocol’s scope.

KEY POINTS

1. Co-developed by twenty-one companies across three verticals, UCP keeps the business as Merchant of Record at the checkout, and the rival protocol keeps the merchant as system of record for orders, payments, taxes and compliance.
2. A merchant that authorises an agent-hosted feed holds one hosted copy of its catalogue per agent, each with its own feed id and update timestamp.
3. Returns and exchanges are outside the draft protocol's scope while the merchant stays system of record, so the party that keeps the return is not the party that keeps the record.
4. The right to complete a checkout without a buyer present comes from the platform's trust tier, not from the merchant.
5. Four filings between 20 October and 4 November 2026 put the same position on opposite sides of the table: one lender took a design-partner seat in a protocol initiative, a second announced integrations with the platform and released a framework of its own, a third named agentic commerce as a threat to demand from its brand partners, and a merchant put it on a slide with no figure.

The protocol that twenty-one companies co-developed across shopping, lodging and food now says who pays when an agent's order goes wrong, and it is the seller. Co-developed by Google, Shopify, Etsy, Wayfair, Target, Walmart, Amazon, Microsoft, Meta, Salesforce and Stripe on the shopping tab alone, in the site's own words, UCP keeps the business as Merchant of Record at the checkout. The Agentic Commerce Protocol, maintained by OpenAI and Stripe and labelled beta, keeps the merchant as system of record for orders, payments, taxes and compliance, and puts returns, exchanges and fraud modelling outside its own scope. What moves is everything else. The catalogue is served from an agent-hosted feed, the price a buyer sees is a record on that feed, and the platform's trust tier rather than the merchant's own limits decides which agents may complete a sale unaided. This reaches you if you take payment on your own rails and carry Merchant of Record liability on orders an agent assembled without you, which puts the FY27 catalogue budget in front of you before 31 March 2027.

The platform decides who may finish the sale

Shopify's developer documentation walks an agent through the whole purchase and names what trust buys. Install a command line tool, authenticate, search the catalogue, build a cart, create a checkout, hand the buyer off, track the order: “Higher trust tiers unlock broader access, including direct checkout completion.” The merchant is not the party setting that tier, and the same documentation sells the union of every merchant's stock as one index: “Search products across every Shopify merchant from a single endpoint.” The newest surface is more explicit still, an early access waitlist for “One Cart, every brand. The Universal Cart API lets AI agents collect items from any merchant, on or off Shopify, into a single, unified cart, all via UCP.” A merchant on that cart is one line item in a basket another party owns.

Neither protocol is ambiguous about who carries the result. The Agentic Commerce Protocol's own README, addressed to the agent builder, puts it in the negative: “Let your users discover and transact directly with businesses in your application, without being the merchant of record.” One standard excludes the agent from the liability. The other assigns it to the business. They mean the same thing.

Both protocols put the loss back where it already was

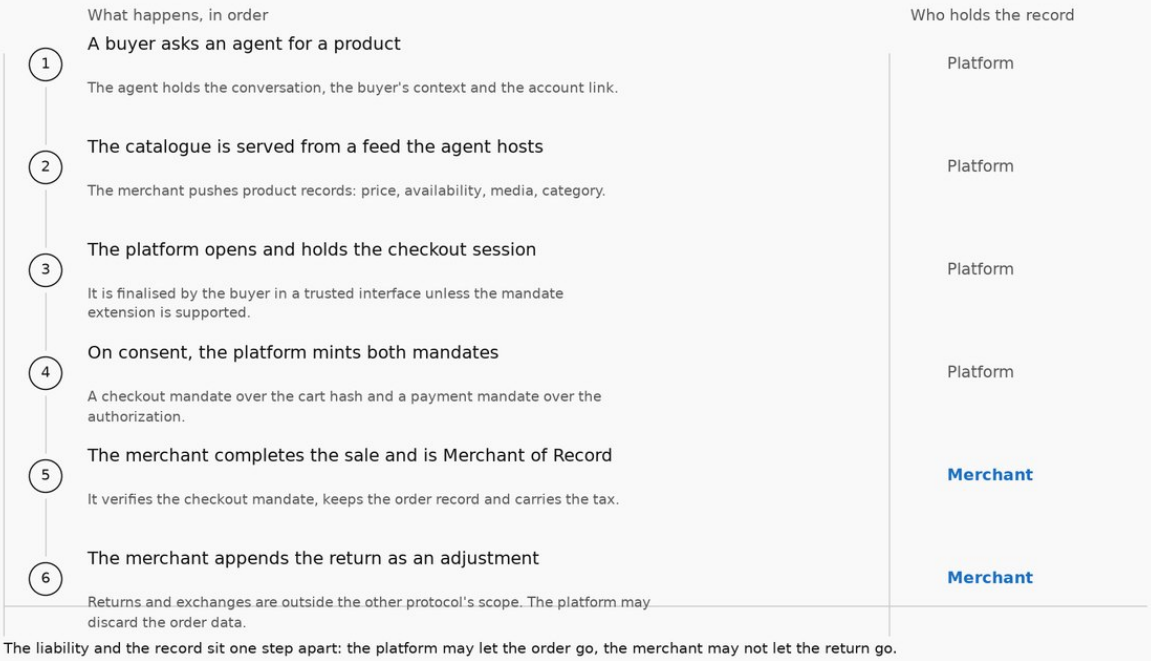
Five things that move, and the party each one leaves holding the cost

The lever	Universal Commerce Protocol	Agentic Commerce Protocol	What it leaves with the seller
The buyer and the cart	The platform negotiates capabilities and holds the session; the checkout is finalised manually by the user unless the AP2 mandates extension is supported	ChatGPT creates, updates, retrieves, completes and cancels the checkout sessions	The order, and the return on it
Merchant of record	“The business remains the Merchant of Record (MoR)”	“The merchant remains the system of record for all orders, payments, taxes, and compliance.”	Financial liability, tax, compliance and disputes
The catalogue	The business publishes a profile and exposes the catalog capability to be searched	The merchant pushes product records to agent-hosted feeds, a surface the changelog heads unreleased	Keeping a copy accurate on infrastructure it does not run
Returns and exchanges	The business appends adjustments; an append-only ledger is preferred	Named out of scope	The whole workflow and the whole cost of it
The order record	The platform should treat order data as ephemeral and discard it when no longer needed	The merchant is the system of record	Possession of the record, and the duty to produce it

Source: Universal Commerce Protocol, ucp.dev, shopping checkout, catalog and order capabilities; Agentic Commerce Protocol, README, rfcs/rfc.agentic_checkout.md version 2026-01-16 and changelog 2026-04-17.

Returns are the merchant's twice, by assignment and by omission

The draft that governs OpenAI's checkout states its own limits in one line: “Out of scope: PSP authorization/capture semantics, returns/exchanges workflows, tax configuration, fraud modeling details.” Those four are not edge cases. They are the four places an order costs money after it is taken, and the same document assigns every one of them to the merchant in the sentence before it. UCP takes the other route to the same place: a return is an adjustment the business appends to its own record, and the guidance to the platform is to forget the order once the flow is done.



Six steps of an agent checkout, in order, and the party holding the record at each one. The record and the liability separate at step 5: the platform may let the order data go, the merchant may not let the return go. Source: Universal Commerce Protocol, ucp.dev, shopping checkout and order capabilities; Agentic Commerce Protocol, rfcs/rfc.agentic_checkout.md version 2026-01-16; Universal Commerce Protocol, UCP and AP2.

The price becomes a record on an agent's feed

The catalogue leaves next, and it leaves as a push. The protocol's changelog describes the surface it heads unreleased: “These endpoints are hosted by Agents and called by merchants. The Feed API is a push model: merchants push product catalog metadata and product records to Agents, rather than Agents pulling catalog data from merchant-hosted endpoints.” What travels in that push is the commercial record: product, variant, price, availability, media, category and seller. The protocol's own RFC concedes the weakness of the copy in the same breath, since “Feed data can be cached, delayed, or scoped for discovery.” A stale price on an agent's feed is a price the merchant no longer controls the display of, and the merchant is the party who has to honour or refuse it.

An unreleased proposal in the same repository goes further, and it is a proposal, not a rule: “Add suggested_price to Item on CheckoutSessionCreateRequest, enabling agents to communicate price provenance to sellers for catalog price matching.” The schema it introduces carries feed_id as a required field, alongside channel, feed_update_id and updated_at. An agent that observed a price on one channel could present it at checkout on another, with a receipt. That is a direct attack on channel price differentiation, and it is one merge away from being operative text.

Four filers priced the same position on opposite sides of the table

What four filers told their own shareholders between 20 October and 4 November 2026

Filer	Filed	What the filing says	Which side of the table it sits on
Synchrony Financial, Form 8-K and Q3 2026 release	20 October 2026	“Established partnership with OpenAI, combining strategic agentic commerce collaboration with enterprise AI access”, and joined the Personal Agent Protocol (“Poppy”) initiative led by Sierra and Meta as a design partner	Inside the room, writing the standard
Bread Financial, Form 8-K and September 2026 credit statistics	22 October 2026	Among the things that could cause “loss of, or reduction in demand for services and/or products from, significant brand partners or customers”: “the emergence or increase in popularity of agentic commerce, digital payment platforms and currencies and other alternative payment and deposit solutions”	Outside the room, holding the demand risk
American Express, Form 8-K and Q3 2026 release	23 October 2026	“The company announced Resy integrations, including with OpenAI, and released the Intent Intelligence framework for trusted agentic commerce.” The same filing's risk factors add “the effects of the emergence of agentic commerce on the payments landscape and customer payment experiences”	Inside the room, and pricing the risk
The Estee Lauder Companies, Form 8-K, Exhibit 99.2	4 November 2026	“Agentic Commerce & Experiences” printed as one of two named items under “NEW CAPABILITIES & GROWTH” in a capital markets deck, with no figure attached	The merchant, naming a capability

Source: SEC filings and exhibits named in each row, filed between 20 October and 4 November 2026.

Read together, the four filings describe positions and not a market. One lender took a design-partner seat in a protocol initiative and listed it under “Business Highlights” in its own release. A second announced Resy integrations, including one with OpenAI, and released a framework of its own for agentic commerce. The lender with no role at all put agentic commerce in the list of things that could take its brand partners' demand away, which is the same risk stated from the other side of the table. The merchant put it on a slide. None of the four gives a volume, a return rate or a loss figure, so nothing here prices the channel. What the filings price is the position: the risk lands on the party whose revenue depends on somebody else's brand partners, and the capability lands on the parties already inside the room.

The mandate proves consent, not who carries the return

Autonomy arrives as a credential the platform mints. Under the mandates extension, “Upon user consent, the Platform generates two credentials”, a checkout mandate containing the hash of the checkout object and a payment mandate containing the payment authorization, and the platform submits both to the business to complete the order. The business then verifies the checkout mandate and the payment processor verifies the payment mandate. That is a genuine improvement in proof of what was agreed, and it is worth having. It is also a document the merchant receives rather than creates, on a sale whose returns the merchant still funds, and the protocol without it is not autonomous at all: the checkout “has to be finalized manually by the user through a trusted UI unless the AP2 Mandates extension is supported.” A merchant that wants the agent's volume takes the platform's instrument with it.

What each seat owes, and by when

Four decisions, four owners, and the fact that forces each one

Seat	What to do	By when	Why this one
Chief digital or commercial officer	Decide in writing whether the product record goes to any agent-hosted feed, and name the agents. A feed is an authorisation, not a setting	31 March 2027, with the FY27 catalogue budget	Each authorised feed is a hosted copy of the catalogue with its own id and update timestamp, and the price a buyer sees is a record on it
CFO	Put a per-order return and dispute cost against the agent channel in the FY27 plan, and state what share of the return the channel carries	31 March 2027	The draft protocol names returns and exchanges out of scope while leaving the merchant as system of record, so the provision is unchanged and the sale is new
General counsel	Read the merchant of record clause in every agent platform agreement before signature, and require that it match the allocation the protocol already states	Before the first feed is authorised	Both protocols put the liability on the seller, and a contract that is silent on it inherits that default
CIO	Pin the UCP version in the business profile and record which versions the business declares it supports	30 June 2027, ahead of the next release branch	A breaking change is announced two weeks before it merges, and a version the business does not support is refused with version_unsupported

Source: Mosaic Singularity analysis, November 2026, drawn from the protocol specifications, Shopify's developer documentation and the four filings cited in this piece.

One date in that table is set by the financial calendar rather than by the protocol. The chief digital or commercial officer and the CFO both sign into the FY27 plan by 31 March 2027, which is the last point at which the feed decision can be taken without a mid-year re-forecast; the general counsel's merchant of record clause then belongs in the first agent agreement that reaches signature, because the default is already written. That makes it a board decision by 31 March 2027: the FY27 plan carries the catalogue budget and the per-order return provision in one approval, so a board that passes the plan with a feed authorised and no stated return cost per agent-originated order has approved the sale and deferred the loss.

The questions a board should put to management

- Which agents can complete a sale on our behalf without a buyer present, and who granted that right: the platform's trust tier or our own limits?
- Where does our product record now live, on whose feed, and who is accountable when the copy goes stale and a buyer is charged the wrong price?
- What is our return rate on an agent-originated order, and does anything in the channel carry any part of it?
- When a dispute arrives, what do we hold? The mandate is generated by the platform and verified by the processor, not created by us.
- Does the merchant of record clause in each agent agreement match the sentence the protocol quotes, or does it rely on it?
- Which version of each protocol do we declare support for, and who reads the two-week notice when it comes?

What to watch, and when

- 30 June 2027: the first merchant 10-Q or 10-K to name agent-originated revenue, or the return against it. If none has by then, the reading that this is a channel with a measurable cost fails.
- Any released version of the Agentic Commerce Protocol carrying the suggested price proposal. That is the day channel price differentiation becomes the argument rather than a footnote.
- UCP Lodging and Food: seven co-developers in lodging and five in food against eleven in shopping, on the site's own tabs. Every vertical that ships carries the same allocation into another P&L.
- A protocol revision that brings returns and exchanges into scope and assigns them to the platform. That single change would close the asymmetry this piece describes.
- The next annual reports from the three lenders: whether agentic commerce stays a risk factor or acquires a number, which tells you whether the credit side found the cost before the merchant side did.

Every quotation in this piece traces to these eight documents

Universal Commerce Protocol, ucp.dev: home page, core concepts, shopping checkout, catalog and order capabilities, versioning and roadmap.

Agentic Commerce Protocol, maintained by OpenAI and Stripe: README; changelog 2026-04-17; changelog/unreleased/suggested-pricing.md (SEP #197); rfcs/rfc.agentic_checkout.md, version 2026-01-16, Status Draft; rfcs/rfc.orders.md, rfc.product_feeds.md, rfc.seller_backed_payment_handler.md.

Shopify developer documentation, shopify.dev/docs/agents.

Agent Payments Protocol documentation, via the Universal Commerce Protocol's UCP and AP2 page.

Synchrony Financial, Form 8-K filed 20 October 2026, accession 0001601712-26-000040, and the Q3 2026 earnings release furnished with it.

Bread Financial, Form 8-K filed 22 October 2026, accession 0001101215-26-000088, and the September 2026 credit statistics exhibit furnished with it.

American Express Company, Form 8-K filed 23 October 2026, accession 0000004962-26-000405, and Exhibit 99.1.

The Estee Lauder Companies Inc., Form 8-K filed 4 November 2026, accession 0001001250-26-000066, Exhibit 99.2.