Invisible Coverholders: Agent-to-Agent Commerce Is Delegated Authority Without Disclosure

Invisible Coverholders: Agent-to-Agent Commerce Is Delegated Authority Without Disclosure

Agent-to-agent commerce protocols are starting to move from experiment to infrastructure. Systems are now being designed so software agents can discover each other, negotiate terms, place orders, approve transactions, and trigger financial movements without per-transaction human approval.

The technology story is getting attention.
The underwriting story is not.

From an insurance perspective, this is not primarily an AI story. It is a delegated authority story — but without the disclosure and control structures the market normally requires when authority is delegated.

Insurance already knows how to insure delegated authority. It does it every day through delegated underwriting, delegated claims handling, and binder structures.

What's new is not delegation.
What's new is **delegation to software agents without placement-grade authority description.**

That is where the risk sits.

Insurance Already Has a Model for This — Delegated Authority

When a carrier delegates underwriting authority to a coverholder, the market requires structure:

- defined scope of authority
- transaction limits
- class boundaries
- reporting duties
- audit rights
- authority schedules
- bordereaux trails

The risk is not "someone else made a decision."
The risk is **someone else made a decision within disclosed and bounded authority.**

Now consider agent-to-agent commerce systems.

Software agents are being authorised to:

- select counterparties
- negotiate terms
- approve purchases
- trigger payments
- execute refunds

- commit contractual actions

Functionally, they are acting like delegated operators.

But in most insured environments, this authority is:

- not described at placement
- not classified by autonomy level
- not bounded in underwriting disclosures
- not reflected in proposal answers
- not attached to authority schedules

That gap is where the dispute will form.

The Underwriting Blind Spot: Capability Is Disclosed, Authority Is Not

Current submissions increasingly disclose:

- AI usage
- automation tooling
- model controls
- security controls
- audit logs
- human oversight frameworks

They rarely disclose:

- whether a system can commit transactions without approval
- whether an agent can bind commercial outcomes
- whether agents can spawn sub-agents with inherited permissions
- whether authority thresholds are machine-executed or human-approved
- whether financial decisions are advisory or executable

Two systems with identical models and controls can produce radically different exposure depending on one factor:

Does the system advise — or decide?

That is not a technology distinction.
That is an authority distinction.

A Concrete Claims Scenario

Consider a merchant using an agentic procurement protocol.

An internal commerce agent is authorised to source and place orders under a value threshold. The agent negotiates with supplier agents through an agent protocol layer. A supplier agent misrepresents delivery capability. Orders are placed. Loss occurs.

At claim:

The insured says:
> “The agent made the purchasing decision.”

The insurer asks:

- Was autonomous purchasing authority disclosed?
- Were value limits declared?
- Was agent authority bounded in the submission?
- Was this advisory automation or execution authority?

If the placement record describes “AI-assisted procurement tools” but not **autonomous purchasing authority**, the dispute is no longer about model error.

It is about disclosure.

Not:
> Did the system fail?

But:
> Was the authority it exercised declared?

Recursive Agents Do Not Remove Delegation — They Move It Upstream

A common objection is emerging quickly:

“What if agents create other agents? What if tracing delegation is difficult?”

From a claims perspective, recursive autonomy does not eliminate delegation. It shifts the delegation question upstream.

When tracing is difficult, claims does not stop. It asks different questions:

- Who enabled the system to operate externally?
- Who granted financial permissions?
- Who set authority thresholds?
- Who allowed autonomous execution?
- Who failed to bound replication or escalation rights?

This is not absence of delegation.
It is delegation by design.

Liability does not disappear when the chain becomes complex.
It **consolidates upward** to whoever enabled unbounded authority.

Not All Agents Are the Same Risk

Underwriting needs a simple classification distinction that is mostly absent today:

- **Advisory agents** — recommend, humans decide
- **Approval-gated agents** — act after human confirmation
- **Bounded autonomous agents** — act within fixed limits
- **Self-directing agents** — adapt scope and spawn actions

Most proposal forms treat these as one category: “AI used.”

They are not one category of risk.
They are different delegated authority classes.

If the authority class changes, the disclosure obligation changes.

The Placement Test

A practical underwriting test:

If a human previously approved each transaction and now a system approves within limits — and the proposal form answer did not change — delegated authority has shifted without disclosure.

That is a placement fact.

Not a technical detail.
Not an implementation nuance.
A placement fact.

Where Coverage Fights Will Actually Form

In agentic commerce losses, disputes are likely to cluster around:

- non-disclosure of autonomous authority
- misclassification of advisory vs executable systems
- authority scope exceeding described controls
- absence of authority limits in proposal answers
- wording built for tools applied to delegates

The argument will not stay technical for long.

It will move quickly to:

- scope of delegated authority
- disclosure sufficiency
- authority limits at placement
- whether the insurer priced the authority actually exercised

---

What Underwriters Can Do Now

Three immediate underwriting adjustments:

1. Ask the authority question directly

Not “Do you use AI?”
Ask:

> Can any system commit financial, contractual, or operational decisions without per-action human approval?

2. Require authority descriptions

For agentic systems:

- decision types
- value limits
- escalation triggers
- override controls
- replication rights

3. Treat agent authority like delegated underwriting

If authority exists, require:

- authority schedules
- limit structures
- scope boundaries
- auditability

Human or code — authority is still authority.

The Core Principle

Insurance is not surprised by automation.

Insurance is surprised by **undisclosed authority.**

Agent-to-agent commerce is not primarily a model risk.
It is a delegated authority risk.

And delegated authority that is not made explicit at placement will be reconstructed later — by claims counsel, underwriters, and courts — under pressure.

Better to classify it before the loss than argue it after.

Authority transferred is authority insured.