

The Automotive Stack Is Exposed, and Not Just to the FTC

Automotive spent years connecting the customer journey. AI is turning those connections into actions. What the stack still hasn't connected is authority.



THOMAS ROCHA III

OCT 08, 2026

The Automotive Stack Is Exposed, and Not Just to the FTC

*Automotive spent years connecting the customer journey.
AI is turning those connections into actions.
What the stack still hasn't connected is authority.*

THOMAS ROCHA III

ON SUBSTACK
OCTOBER 2026



In February, I published a glossary with an argument.

The glossary collected the words that different industries use for failures they can observe but cannot fully control. The argument was that the words describe one thing. I called them the Seven Convergent Failure Domains: accessibility, zero trust, AI coordination, data residency, mobile networks, the efficiency paradox, and concurrency

control. Seven fields, seven vocabularies, and underneath them the same event. Something changes inside a live interaction, and nothing guarantees that the authority governing it survives the change.

That was not an argument about cars.

It was not new in February, either. I have been reducing that relationship to an architecture and an evolving patent family since 2024. The first patent in the family issued this June. That is not an assertion that any particular company practices any particular claim. It is why the convergence matters to me. I watched seven fields arrive at the same problem from seven directions.

Now I am watching one industry arrive at all seven at once.

The Seven have arrived at the dealership

In August, I argued that an FTC settlement can close the counts that were charged without closing the architecture that produced them.

The problem was larger than deceptive advertising or unwanted add-ons. A modern vehicle transaction moves through listing sites, incentive feeds, dealer websites, chat systems, payment tools, trade applications, call platforms, CRMs, DMSs, finance systems, analytics, AI, and people. Each system can keep an accurate record of what happened inside its own walls while nobody maintains one authoritative account of what the customer was told, what the customer permitted, and who was entitled to make the next consequential decision.

The obligation attaches during the interaction.

The evidence scatters after it.

Since then, the industry has moved quickly toward what looks like a solution.

Unify the data. Reduce the number of systems. Create one customer record. Put AI over the top. Let the agent act.

One major automotive platform is combining marketplace behavior, CRM history, DMS records, service activity, and purchase history. Another has introduced a customer data platform specifically to unify information scattered among dealership systems while adding agentic AI. Another built a common AI data layer and describes its assistant as moving from question to action. Another describes its destination almost perfectly: one platform, one database, one truth, with AI at the center. Specialist AI companies are answering customers, changing channels, scheduling appointments, updating records, handing conversations to people, and operating according to dealership rules.

They have correctly diagnosed fragmentation.

But they are solving the visible layers of it.

A unified customer record can solve data fragmentation. A common platform can solve application fragmentation. An orchestration layer can solve workflow fragmentation. An AI agent can solve labor fragmentation.

None of those things, standing alone, solves authority fragmentation.

That's where the seven come in. Automotive is running into every one of them, inside a single ordinary consumer journey.

They look different from one another.

They are increasingly the same problem.

Accessibility changes the interaction

Start with the simplest example.

A shopper begins on a website. They move to chat. Then perhaps video. Then a phone call. Then an appointment. Maybe they need captions. Maybe they cannot use voice. Maybe they require a particular communications accommodation.

The industry traditionally treats accessibility as a property of each component. Is the website accessible? Is the form? Does the video support captions? Can the call center handle the customer?

Those are necessary questions, but they are local questions.

The harder one appears when the customer crosses from one system to another:

Did the customer's accessibility state survive the crossing?

If someone establishes a communication requirement at the beginning of an interaction, the dealership should not have to rediscover it at every handoff. Nor should the next system be free to ignore it just because it didn't originate there.

The medium changed.

The governing condition did not.

That is the first version of the problem.

Zero trust reaches its limit at access

Automotive is also rapidly adopting the language and machinery of modern security. Users authenticate. Roles are assigned. APIs have permissions. Applications receive tokens. Agents get scoped access to CRM records, inventory, scheduling and communications systems.

All useful.

But identity is not authority, and neither is access.

An AI agent can be perfectly authenticated and still not be entitled to take a particular action. It can have valid credentials to the CRM, API access to the scheduler, and permission to read the customer record. It can technically possess everything required to book an appointment, send a message or change a lead state.

None of that answers whether it was permitted to perform this action, for this customer, in this undertaking, under the authority presently governing it.

One automotive system already allows authorized personnel to change whether AI may continue participating in an individual conversation. A human can take over while the conversation remains the same conversation. Status and actors can change without discarding the underlying history.

That is no longer really an authentication problem.

It is an authority problem.

The system now has to know not simply *who you are*.

It has to know *what you are still allowed to do*.

AI coordination makes the hidden problem visible

Now add multiple agents.

One communicates. One searches inventory. One handles scheduling. One evaluates a trade. One retrieves finance information. One determines when to escalate. A human joins. Another department takes over. The customer moves from text to voice.

None of this is futuristic. Automotive products already advertise versions of it. Some agents operate under dealership-specific rules while making appointments directly in live dealership systems. Some

preserve conversational context across channels. Some change strategy, timing, and medium while continuing the same commercial objective. Some hand control from machine to person.

The engineering question is usually framed as orchestration: which agent should act, which tool it should call, what information it should receive, where the workflow goes next.

But there is a question underneath all four:

When execution changes, what keeps the governing authority from changing with it?

The customer gave permission to one thing. The dealership authorized another. The manufacturer controls an incentive. The lender owns credit terms. The AI vendor controls some of the agent's behavior. A workflow engine may coordinate them all.

Coordination does not merge those authorities.

A baton can pass between runners without changing the race.

The question is whether authority can do the same.

Data sovereignty turns geography into another mutation

The same customer interaction may touch a dealership, OEM, cloud platform, AI provider, analytics service, CRM, DMS, lender, transcription service, and outside processor. For an international dealer group, it may also cross national borders.

Again, the industry's first question is usually infrastructural. Where is the data stored? Which cloud processes it? Where is the model running?

Those matter. But geography is only one part of sovereignty.

The deeper question is whether the authority associated with the data survives when the data moves.

Permission to collect information does not necessarily authorize every subsequent use. Permission to contact a customer does not automatically authorize another purpose. Authority to use information within one jurisdiction does not necessarily mean it can be transferred elsewhere. A processor receiving the record does not necessarily inherit every right the supplying party possessed.

The bits cross the boundary easily.

The legal and operational authority governing the bits may not.

Omnichannel is a transport triumph

Automotive loves the word omnichannel. And fairly so.

The customer can begin on a marketplace, continue on the dealer website, move into chat, receive a text, make a phone call, watch a video, schedule an appointment, and eventually appear physically at the dealership.

From the consumer's perspective, it may all be one undertaking: *I am trying to buy or service a vehicle.*

The infrastructure sees something very different. An HTTP session. A chat session. An SMS thread. A voice call. A CRM record. An appointment. A deal record. Each has its own identifiers, storage, and technical boundaries.

The industry's achievement has been making those transitions increasingly invisible to the customer.

But transport is not authority.

A communications system that can continue the conversation does not ensure that every permission, restriction, representation, and commitment survives the move correctly.

A new channel should not silently create a new throne.

The customer's work continued. Whatever legitimately governed that work must either continue with it or be explicitly changed.

Efficiency creates its own paradox

This is where the industry's current consolidation push becomes particularly interesting.

The answer to fragmentation is increasingly one platform, one database, one customer, one AI layer. That can produce enormous benefits.

It also changes the failure mode.

In yesterday's badly integrated dealership, a mistaken action might die at a system boundary because the systems could not communicate. The CRM did not know what the website knew. The scheduler did not know what chat promised. The call center could not see what happened online.

Those seams were inefficient.

They were also, accidentally, firebreaks.

Now remove them. Give an AI agent access to the customer history, inventory, service state, communications record, scheduling tools, and dealership rules. Let it act.

The efficiency problem disappears.

The blast radius grows.

A mistake that once died at the boundary can now move from conversation to record to scheduling to follow-up to another system at machine speed. The better the architecture becomes at preserving work, the more important it becomes that it preserve authority just as well.

That is the efficiency paradox.

One database can produce one operational truth. It cannot automatically produce one authority, because there is no single principal. The manufacturer may control one fact. The dealer another. The lender another. The customer controls their own permissions. A regulator may impose a limitation that belongs to none of those parties.

Putting everything in the same database does not merge those sources of authority any more than putting several bank accounts on the same screen merges their ownership.

Then concurrency arrives

Now imagine the same transaction with a human salesperson, an AI agent, a service agent, a follow-up automation, and a customer all capable of acting at approximately the same time.

This is not theoretical either. Some automotive workflows already instruct dealership personnel to disable AI participation before taking over a conversation.

Why?

Because two actors can otherwise continue operating against the same customer state.

At the harmless end, two systems book the same appointment. A little further down the road, an AI quotes something after a salesperson has changed it. A human honors an opt-out while automation continues

marketing. One system revokes permission while another has already queued the next action.

The familiar version of this problem asks which change wins when two collide.

Autonomous systems add a second dimension. It is no longer merely *which state change wins?*

It is *which actor had authority to make the state change at all?*

That is the seventh problem.

And now the seven begin to collapse into one.

Accessibility changes the modality. Zero trust changes the permitted actor. AI coordination changes the executor. Sovereignty changes the permissible location or use. Network complexity changes the transport. Efficiency increases the distance an action can travel. Concurrency changes who can mutate the state.

In every case, something changes inside an undertaking while something else must remain governing.

What authority survives the change?

That is the common question.

When something goes wrong, the seamless journey develops seams

This brings us back to the enforcement problem.

The automotive industry has an interesting habit. Before the transaction goes wrong, everyone sells integration. Seamless journey. Unified customer. Connected retail. One platform. One truth.

Then something goes wrong, and the architecture becomes remarkably fragmented.

The dealer says the number came from a vendor. The vendor says it displayed information supplied by the dealership. The dealership says the incentive originated upstream. The upstream source says the eligibility condition was correct and somebody else applied it incorrectly. The AI company says the dealer configured the rules. The dealer says the AI generated the statement. The platform says it only transmitted the data.

The customer says, quite reasonably:

I don't care. You told me this.

That is where regulatory responsibility collides with distributed architecture. The FTC cases exposed an early version of it. The customer-facing operator could not necessarily escape responsibility simply by pointing to another participant in the chain, and responsibility can extend to multiple participants where multiple participants exercised control.

The finger-pointing is therefore not incidental.

It is evidence.

The industry's architecture makes it difficult to say who owned the act when it occurred, so everyone tries to establish who owns the failure afterward.

Responsibility is reconstructed after the failure. Authority has to exist before the act.

Contracts can divide responsibility. Indemnities can move money. Logs can identify machines. Audit trails can show events. Depositions can determine who configured what.

None of those things retroactively creates the authority that should have governed the action before it happened.

A liability chain assembled afterward is not an authority chain governing the transaction.

Nobody had to be wrong

This is not an accusation, and it is not about any one company.

Most of these systems are sophisticated. They were built to solve real problems. Move the customer faster. Reduce duplicate entry. Connect systems. Personalize communication. Automate routine work. Give employees better information. Make the AI useful.

Every local decision makes sense.

What the public descriptions show is authentication, contractual permission, data access, workflow rules, monitoring and logging. Those carry real pieces of authority. What they do not yet show is the thing that holds those pieces together when the work moves from one system, company or agent to the next.

The gap appears only when you stand far enough away to see that all those locally correct systems participate in one continuing undertaking.

That is why an informed automotive reader can probably identify several companies while reading this without a single logo appearing on the page.

It is also why naming them would miss the point.

There is no villain to identify.

It is the state of the industry.

Automotive is a particularly good place to see it

Automotive did not invent this problem. It simply concentrates an unusual number of its forms into one ordinary consumer journey.

A vehicle transaction can involve accessibility, privacy, identity, advertising, recording consent, AI output, finance, credit, payments, data sharing, communications rules, cross-border processing and eventually physical action. It crosses people and machines, companies, channels and legal regimes. It can begin with an advertisement and end with a signed contract, a loan, a vehicle or a service action.

And the operator standing at the edge may be accountable for a journey whose architecture it does not own.

That was already visible before the current AI wave. The earlier problem was that the customer interaction moved while the proof stayed behind.

AI changes the stakes.

The agent can increasingly move too. It can carry context from one stage to another, call tools, modify records, change channels, act under dealership rules, hand the customer to a person and take the person back. It can continue working past a system boundary that once would have stopped the process.

The industry's original architecture problem was fragmentation.

Its next one is authority at scale.

The primitive underneath the seven

The seven keep collapsing into the same question for a reason.

They are not seven products. They are not seven compliance categories. They are seven different pressures acting on a distributed system, and each introduces a mutation. Media changes. Actor changes.

Agent changes. Jurisdiction changes. Network changes. System changes. Authoritative state changes.

The implementation details can be completely different.

The invariant is not.

An undertaking exists. Something inside it changes. Before that change becomes authoritative, the system must determine whether the governing authority permits it.

If it does, the work continues.

If it does not, the change does not get to become the new truth merely because a tool was technically capable of making it.

And whatever happens needs to remain provable afterward.

That is the relationship the patent family was built around, long before it had a dealership in it.

It is also much closer to the missing layer than another dashboard, another consent database or another giant platform.

The industry already knows how to authenticate actors. It knows how to transport data. It knows how to log events. It increasingly knows how to coordinate autonomous agents.

What it has not yet learned to do consistently is keep the authority governing the undertaking intact as all of those things mutate.

That is why the finger-pointing matters so much. When nobody can prove who authorized the act, everyone is left arguing about who should be responsible.

The future system should answer the earlier question first.

Who is entitled to make this change, here, now, under the authority governing this interaction?

Automotive is beginning to ask that question because it has little choice.

Soon it will have to answer it at machine speed.

And once it does, the seven stop looking like seven different problems.

They look like seven ways of discovering the same primitive.