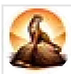
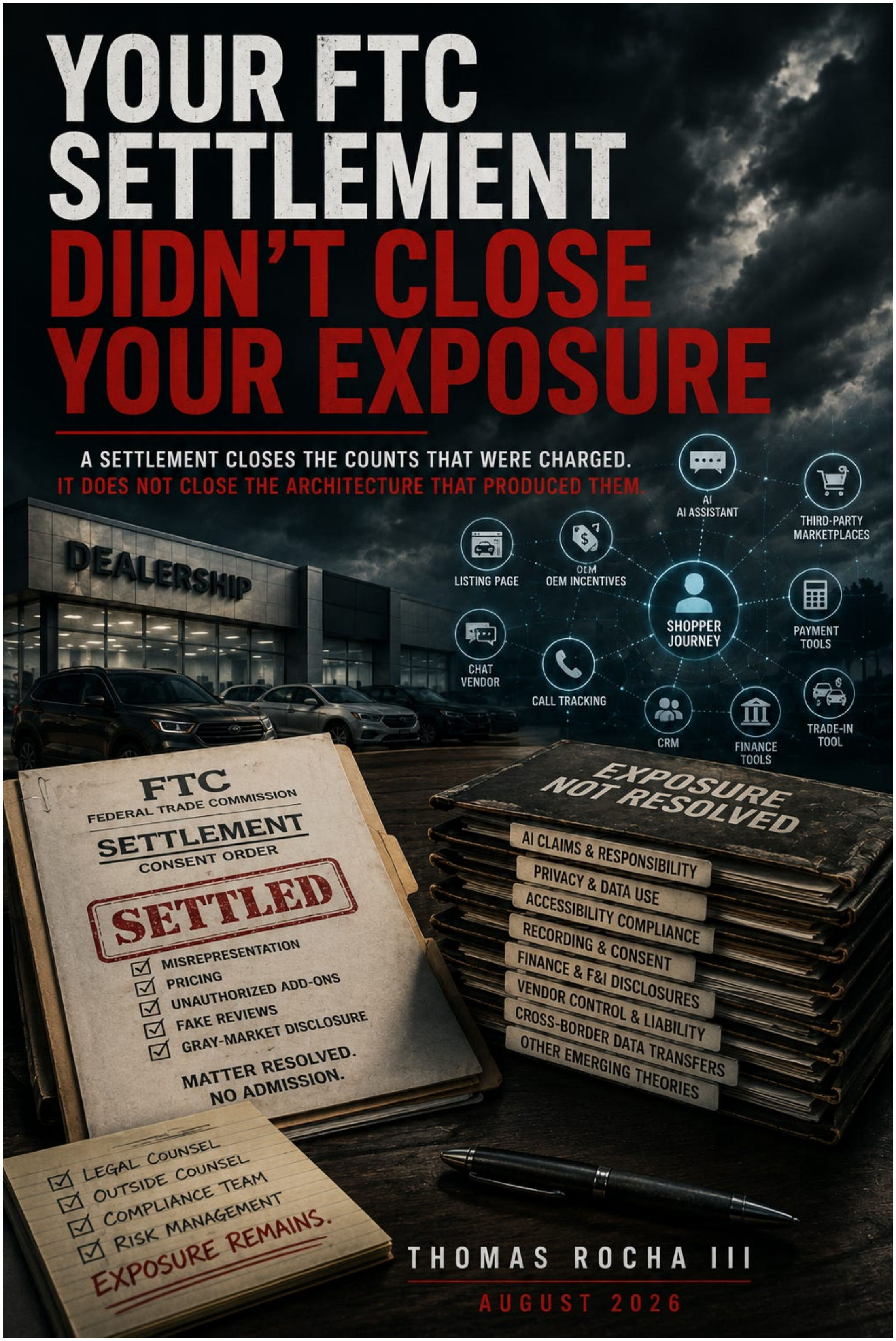
Your FTC Settlement Didn’t Close Your Exposure

A settlement closes the counts that were charged. It does not close the architecture that produced them.



THOMAS ROCHA III

AUG 05, 2026


YOUR FTC SETTLEMENT
DIDN'T CLOSE YOUR EXPOSURE
A SETTLEMENT CLOSES THE COUNTS THAT WERE CHARGED.
IT DOES NOT CLOSE THE ARCHITECTURE THAT PRODUCED THEM.
DEALERSHIP
AI ASSISTANT
THIRD-PARTY MARKETPLACES
LISTING PAGE
OEM INCENTIVES
SHOPPER JOURNEY
PAYMENT TOOLS
CHAT VENDOR
CALL TRACKING
CRM
FINANCE TOOLS
TRADE-IN TOOL
FTC
FEDERAL TRADE COMMISSION
SETTLEMENT
CONSENT ORDER
SETTLED
MISREPRESENTATION
PRICING
UNAUTHORIZED ADD-ONS
FAKE REVIEWS
GRAY-MARKET DISCLOSURE
MATTER RESOLVED.
NO ADMISSION.
EXPOSURE NOT RESOLVED
AI CLAIMS & RESPONSIBILITY
PRIVACY & DATA USE
ACCESSIBILITY COMPLIANCE
RECORDING & CONSENT
FINANCE & F&I DISCLOSURES
VENDOR CONTROL & LIABILITY
CROSS-BORDER DATA TRANSFERS
OTHER EMERGING THEORIES
LEGAL COUNSEL
OUTSIDE COUNSEL
COMPLIANCE TEAM
RISK MANAGEMENT
EXPOSURE REMAINS.
THOMAS ROCHA III
AUGUST 2026

The Federal Trade Commission appears to be cleaning up car ads.

But the enforcement record points to something larger.

If you are in this business, you know about the March 13 warning letters. Ninety-seven dealership groups put on notice that an advertised price has to include every mandatory fee the customer will actually pay. The letters were careful warnings, not findings, no determination that anyone broke the law. Most of the industry read them, adjusted some ad copy, and moved on.

That was the visible surface. Behind it is the enforcement version of the same problem, and that one has teeth.

You know the enforcement record, so I will be quick with it. Leader Automotive Group and its parent AutoCanada settled with the FTC and Illinois in December 2024 for $20 million, then the largest judgment ever against an auto dealer, over pricing, unauthorized add-ons, fake reviews, and gray-market disclosure. Worth noting how the defendant framed it: monetary relief, no admission, matter closed. Even the record judgment resolved without anyone establishing, shopper by shopper, what each consumer was actually shown.

Sixteen months later, Lindsay Automotive Group settled with the FTC and Maryland over the same playbook of low advertised prices and fees added during the process. The number that matters: exposure moved from Leader's $20 million judgment to a Lindsay settlement addressing more than $75 million in consumer charges, plus a separate $3.1 million civil penalty. The penalty model is escalating, and you already knew that from your own inbox.

Asbury broadens it further: payment packing, unwanted add-ons, and alleged discriminatory treatment of Black and Latino consumers at three Texas dealerships. Asbury's issues and determination remain unresolved;

nothing proven. But the shape matters before it resolves, because of where it points.

Put the three together and, taken operationally, the enforcement record points toward something much harder to comply with than cleaner ads.

The transaction the consumer was shown online, in chat, through the payment tools, in the finance office, must match what the consumer was actually told, at every step, across every system that touched them.

That is not an advertising requirement. It is an authority requirement: at every step, someone has to have been authorized to make the representation the consumer received, and that authorization has to hold as the interaction moves. The current legal response cannot satisfy it, because the response operates on obligation and the failure lives in architecture.

That is the real axis, and it is worth stating plainly before going further. The contrast is not paper versus digital. Settlements are not paper; they are legal instruments. The vendor systems are not simply digital; they are distributed. The contrast is obligation versus governance. Law can define what must be true. It cannot, by itself, govern what is allowed to happen across a live interaction that crosses systems, actors, and principals. When this piece calls a settlement a “paper answer,” that is shorthand for an obligation imposed on an interaction no one is governing, not a claim that the instrument is primitive.

The paper answer

A settlement can require a dealer to stop misrepresenting prices, disclose terms, preserve records, train employees, monitor conduct, and report compliance. That may be legally necessary. It does not solve the operational problem, because the shopper interaction is not a paper file.

It is a distributed digital event.

One shopper journey can pass through a listing page, an OEM incentive feed, a website provider, a third-party marketplace, a chat vendor, an AI assistant, a payment calculator, a trade-in tool, a finance prequalification tool, a call tracker, a CRM, a follow-up platform, and a layer of analytics and retargeting pixels.

The missing piece is not a better record of what happened. It is someone standing behind each claim as the interaction moves. Every consequential thing the customer is shown a price, an incentive they supposedly qualify for, a payment figure, an answer from your chat AI, a consent box has to trace back to whoever was actually authorized to make it, and that authorization has to hold when the customer moves from your website to your chat vendor to your call center to the F&I office. When the handoff happens, and nobody is still standing behind the claim, it becomes an orphan: a representation the customer received that no one authorized. And the defaults run the wrong way. Logging in is not the same as being authorized. Having access to the OEM incentive feed is not the same as being cleared to tell this customer they qualify. A number your AI generated is not automatically a statement your store stands behind. A new phone call does not inherit the consent from the website session. When it is unclear whether a claim was authorized, the safe assumption is that it was not, and today's systems assume the opposite.

What it cannot do is establish what was true at the moment the shopper saw the claim, clicked the button, talked to the AI, granted consent, received a payment estimate, viewed an incentive, disclosed personal information, requested an accommodation, or got the follow-up text.

The obligation attaches during the interaction.

The evidence scatters after it.

That is the digital proof gap, and every item below is a different room in the same house.

The front door, and the rooms behind it

The FTC issues are the front door. Pricing, mandatory fees, add-ons, whether the advertised claim survives to the point of sale. The proof burden there is already more than “what did the ad say.” It is what did this shopper see, when, fed by what data, which fees were mandatory, what changed before contract, and who controlled the content.

Now open the doors behind it.

Third-party vendor control. NADA’s own guidance tells dealers to consult website providers, OEMs, lead providers, and qualification tools when addressing tracking issues. That is the architecture problem stated by the industry’s own association: the dealer is responsible for an interaction it does not fully operate.

Privacy, pixels, and lead sharing. Dealer sites collect and transmit shopper behavior through cookies, pixels, lead forms, chat tools, and retargeting systems. The question is not whether a privacy policy exists. It is what data was collected, what notice applied, what consent state existed, which vendor received it, and for what purpose. A policy does not prove the execution state of one interaction.

ADA and digital accessibility. If the forms, chat, video, finance tools, and disclosures are not accessible, the exposure is not a bad accessibility score. It is potentially unequal access to the dealership’s goods and services. A general ADA policy does not prove that this shopper received an accessible interaction at the moment they needed it.

AI-generated claims. This is the one that changes the size of the problem. When an assistant quotes a payment, describes availability, explains an incentive, or summarizes a trade under the dealer or OEM brand, that output becomes part of the consumer-facing transaction. The FTC, DOJ, CFPB, and EEOC have all said the same thing: there is no AI exemption from existing law. So the proof question becomes what prompt, what data, what answer, what disclaimer, which model, whether a human reviewed it. “The AI is monitored” does not prove what the AI told the shopper.

Recording and capture consent. Voice, video, call recording, transcription, sentiment analysis. What did the shopper authorize, at what point, for which medium, for which downstream use? A consent checkbox is worthless if the system cannot bind that consent to the actual captured interaction.

Finance, credit, and trade representations. Payment calculators, prequalification tools, trade widgets, lender offers, protection products. Each creates consumer expectations about price, affordability, and eligibility. What payment was shown, on what assumptions, with what fees, from what lender, under what disclaimer, and did the final terms deviate. This is exactly where a paper settlement struggles, because the issue is not whether finance staff were trained. It is whether the system can prove the digital path that delivered the shopper into finance.

Cross-border data transfer. The non-US version of the same thing. Automotive groups and OEMs are international; their vendor stacks are global. If shopper data moves through cloud, analytics, AI, or transcription outside the origin jurisdiction, someone has to prove the transfer carried equivalent protection. A data processing agreement does not prove the path of a specific record through a multi-vendor stack.

Eight rooms. One defect. In every one of them, the obligation is evaluated at a moment inside the interaction, and the proof is expected to be assembled afterward from systems that were never built to produce it.

Why the proof scatters

Every one of those systems can perform its job. The listing renders. The calculator returns a number. The chat vendor answers. The CRM logs the lead. The pixel fires. Each is locally correct.

What none of them does is carry, across the whole journey, a continuous record of what the shopper was told and what they authorized, bound tightly enough to prove it later.

The dealer can prove the ad existed. The website provider can prove the page loaded. The chat vendor can prove a session occurred. The lender can prove an application was submitted. The AI vendor can prove the model returned a string. Every record is real. The assembled journey still has no single defensible answer to the operational question a defensible consumer-interaction system should be able to answer:

What was this specific shopper told, and what did they agree to, as the interaction moved from first claim to signed contract?

Logs show that events happened. They do not, by themselves, show that the same governed interaction survived from the advertised price to the finance office with its representations and consents intact.

And there is no single authority to point to, because there is no single principal. The OEM authorizes the incentive, the dealer sets the price, the lender owns the credit terms, the marketplace owns the display, the AI vendor generates the language. So the decisive question is not “who controlled the content.” It is which principal authorized which actor to perform which act, within which interaction. No system in the stack answers that, because no system in the stack can see all of it.

The claim was made during the interaction. The interaction moved. The proof stayed behind.

Why the exposure is disproportionate

This is not because car dealers are uniquely dishonest, and it is not because automotive got here first. It didn’t. Max Schrems has been litigating fragmented digital authority against Facebook and Meta since 2013. That campaign produced structural judgments at the largest possible scale: a €1.2 billion EU data-transfer fine in 2023, the biggest in GDPR history, on top of hundreds of millions in other Irish GDPR penalties, and a separate $5 billion FTC penalty in 2019. The architecture problem was exposed at platform scale a decade ago.

But Meta is a multinational with tens of billions in annual revenue. Those penalties, enormous in absolute terms, land on an enterprise built to absorb, appeal, and operationalize them. Meta can build interaction-level compliance architecture once and spread it across billions of interactions.

Lindsay is categorically different. A regional dealership group faces refund exposure tied to more than $75 million in consumer charges, plus a $3.1 million civil penalty, and has to prove, refund, remediate, and operate under the resulting order across a vendor stack it does not own. That is the real exposure. Not the scale of the penalty. The scale of the penalty relative to the operator carrying it, and relative to that operator's ability to control the architecture that produced it.

Severity can be measured three ways: absolute penalty size, penalty relative to revenue, and the cost of proving, refunding, remediating, and operating under the order. Meta dominates the first. A dealer group can be more exposed on the third, and that is the one that matters here, because it does not depend on a ratio anyone can argue about. Schrems exposed the architecture problem at platform scale. Lindsay shows what happens when platform-scale regulatory expectations reach businesses without platform-scale balance sheets.

That gap is structural. A single car purchase touches pricing law, privacy law, accessibility law, recording-consent law, AI-output liability, finance and credit representation, and cross-border data transfer, in one interaction, through a dozen vendors the dealer is accountable for but does not control, in a high-value transaction that runs from an online ad to a signed retail contract. The interaction-level evidentiary expectation is the same one now aimed at platforms. The capital, technical control, data governance, and bargaining power are not. The dealer is accountable at the edge while the architecture is owned elsewhere.

Automotive is not the last place this shows up. It is the clearest early one, because it stacks the most regulated surfaces into the highest-value everyday consumer transaction and hands the bill to operators who did not build the stack and cannot compel it to cooperate. Every other vertical that runs a consumer through a distributed digital interaction is walking the same way: retail finance, insurance, healthcare intake, travel, anything with an AI front end, a payment tool, a consent requirement, and a vendor stack it does not own.

The settlement does not close the architecture

Look closely at what a settlement does and does not do. It does real work: Leader's order requires offering-price disclosure and consent for charges; Lindsay's imposes price and consent requirements and provides for consumer redress. Those are meaningful. But look at what they resolve. Leader settled pricing, add-ons, fake reviews, and gray-market disclosure. Lindsay settled advertised price and unwanted add-ons. Those are the counts that were charged. They are not the surfaces that exist.

The same dealerships that settled those counts still run privacy pixels, chat tools, AI assistants, recording, finance widgets, and cross-border vendor pipes, none of which were in the complaint and none of which the settlement touched. A settlement can remediate the charged practices without repairing the cross-system architecture that let representations, consent, and state fragment in the first place. It can prohibit conduct, mandate disclosures, require consent, and impose monitoring, and still leave the interaction itself ungoverned across the boundaries between vendors. Resolving the named issues does not shrink the exposure so much as itemize it. "We settled" means "we are clear on the four things they happened to name this time," in a house with eight rooms.

Why the full stack does not save you

The reflex, reading all this, is to reach for the biggest possible vendor. Consolidate the whole journey inside one unified platform, one record, one throat to choke. The platforms have made exactly this pitch for years, and they will read this enforcement wave as vindication. Adopt the whole stack and the problem disappears.

It does not disappear, for a reason no amount of module-buying can fix. The dealer is not in the platform’s stack. The OEM is not in the platform’s stack. The incentive that seeds the claim comes from the manufacturer. The contract that has to honor the claim is signed at the dealer. The platform sits in the middle and can instrument only the middle. A unified vendor produces a locally complete record of the part it owns and still cannot close the loop across the two parties who actually make and honor the representation. Full stack is a coverage claim about one company’s software. It is not an authority claim about the interaction. It is the same fragmentation with a single logo printed on the fragments.

And there is a deeper problem, the one that should stop the platforms before they take a victory lap. Inside their own walls, they are maintaining transport, not authority. A platform that hands the shopper from listing to chat to calculator to lead is moving the interaction across its own modules, competently. That is transport. It is not the same as carrying a continuous governing record of what the shopper was told and agreed to, bound to the state that results. They optimized the pipe, and authority still falls out at the seams between their own components, because those components were built for throughput and handoff, not for authority that survives the handoff. The would-be cure exhibits the disease at higher resolution, and it will be sold as the answer precisely because it is fast and unified, which are transport virtues.

The exposure is not only the dealer’s

It is tempting to read all of this as a dealer problem. The dealer signs the contract, so the dealer answers for it. That is where enforcement lands first. It is not where it stops.

Start with the manufacturer. On January 14, 2026, the FTC finalized a twenty-year consent order against General Motors and OnStar for collecting and selling drivers' precise location and behavior data without meaningful consent. No dealer in that action. The OEM itself was held directly under Section 5 for how data generated in its vehicles was collected and sold. And the harm traveled: GM sold to consumer reporting agencies, who fed insurers, who raised premiums. The exposure propagated down the chain to consumers who never saw the transaction that created it. On the pricing surface, the direction reverses, but the principle holds. The incentive, the rebate, the eligibility rule often originate with the manufacturer and flow down through the dealer's site. When the advertised number is wrong because the incentive feed was conditional or misstated, the representation traces upstream, to the OEM.

Now the vendors. When a chat vendor's AI quotes a payment, when a calculator generates a figure, when a marketplace's pricing display is manipulated, the vendor's system made the consumer-facing claim. The dealer is accountable for it, but the vendor produced it. "No AI exemption from existing law" cuts at whoever generated the output, not only whoever displayed it. A vendor supplying the instrument that makes an unauthorized representation is not obviously outside Section 5, and is squarely inside the indemnity fight the moment the dealer is penalized.

That indemnity fight is the point. Even where a regulator names only the dealer, the dealer's settlement detonates along the contracts: indemnification claims, vendor-agreement disputes, OEM chargebacks, liability flowing to whoever's tool touched the interaction. The exposure travels the same fragmented paths the authority failed to cross.

Authority fell out at the seams; liability now flows through those same seams, in the other direction, to whoever is standing on the far side.

So the dealer is the first to get hit, not the last to pay. The dealer is the visible edge. The vendors and OEMs are the invisible balance of the exposure, and they have spent years treating dealer-facing liability as the dealer's problem. It is not. It is the stack's problem, and it surfaces at the dealer because that is where the contract is signed, not because that is where it ends.

What the paper answer never rebuilds

A settlement can define obligations, punish failures, require policies and monitoring. It cannot rebuild the thing that created the gap: an architecture where authority travels with the interaction instead of dissolving at the seams between systems.

Here is the whole matter in one line. Digital retail learned how to move the customer through the journey and how to keep records of each step. It never learned how to keep one accountable owner standing behind what the customer was told as the journey moves. The industry has tools that verify who logged in, tools that log what happened, and tools that prove which contract is the final one. None of them keeps the customer's whole interaction under a single accountable authority as it crosses from the ad to the website to the chat vendor to the lender to the signature. That is a distinct thing, and it does not yet have a settled name. Call it session authority, or interaction authority. The name matters less than seeing it is its own category, not another dashboard, CRM, or compliance-monitoring tool.

That layer is not a dashboard, a policy binder, or a vendor-consolidation pitch. It is the requirement that what the shopper was told, what they consented to, what was mandatory, and what the AI said each stay bound to the principal that authorized it, and survive every mutation in the interaction, so that what was true can be established afterward by whoever has to answer for it. One instance of it is the architecture I have written about elsewhere as SSOAR, and the broader principle as authority that survives mutation. The reference surface is hermes-echo.com.

A patent does not make anyone FTC-compliant by Tuesday; that would be its own kind of paper answer. The honest claim is narrower. The FTC identified the claim problem. Leader set the exposure baseline and Lindsay moved it well past it. Asbury, if the allegations hold, reaches into finance conduct and discrimination. NADA's own guidance concedes dealers cannot solve it alone, because OEMs and vendors own much of the interaction. None of the current tools close it, not because they are primitive, many are sophisticated systems with identity controls, immutable records, and consent capture, but because each governs only the slice inside its own boundary. The interaction crosses those boundaries without a common authority model that travels with it.

You cannot settle your way out of an architecture problem.

The settlement closed the counts. The exposure is still open, and it is not only yours.