The Operator's Audit

From The Demo Is Dead, Automotive AI Summit, MIT Museum, September 2026

Six questions to ask any AI tool before customer data goes in.



Yuriy Demidko
September 27, 2026
yuriydemidko.com

Anyone can ship a polished AI product now. A dashboard that looks like a funded startup is one paragraph away. A demo that feels like a year of engineering is fifteen minutes of clicking.

I know because I built one. LeadPulse AI: intent scoring on every lead, an assistant trained on your pipeline, dashboards by rooftop, set up in a day. It looked like $2,500 a month. It took one prompt, one file and fourteen minutes, and I did not read a line of the code. The pitch video had no human in it either. Script, voice, music, footage, all AI. Watch the fake pitch on the home page.

Under the hood: the OpenAI key sat in the browser for anyone to copy. One URL with no login returned all sixty customers, with phone numbers, VINs and credit scores. The login screen was a suggestion the server never checked. Debug logging printed the customer list to the console on every page load.

None of that came up in the demo. A demo is the part of the product designed to be looked at.

Polish is not evidence

In 2018 a polished demo meant a funded team, a year of work and something to lose. Today it means someone typed a paragraph. The cost of building collapsed. The cost of being wrong with customer data did not.

Your buying process has not caught up. It still asks for the demo and still trusts the screen. This paper is the replacement: six questions, asked before the data goes in.

Who pays when it breaks

The customer whose data leaked does not care who vibe coded the app, that it was a pilot, or that the vendor was two people in a shared office. They walked into your store and gave their information to you.

The regulator treats a dealership as a financial institution. Under the Safeguards Rule, vendor oversight is your obligation, not the vendor's.

The vendor has no insurance, no security team, and a laptop.

Liability does not transfer with the invoice.

The six questions

1. Where does my data go? Which model provider, which region, retained for how long, used for training or not. Every prompt that carries a customer name, phone or VIN is a data transfer. Consumer AI accounts can retain it and train on it. Business and enterprise API tiers usually do not, but only if someone signed that agreement. Most vibe-coded tools started on a personal account and never left. A tool that cannot answer this in one sentence has not thought about it.

2. Who can see what? Named users, roles per store, multi-factor on every seat, access reviewed every quarter. Authentication is the thing a prompt forgets unless you ask for it, so the tool ships with one shared login and every store's data in one bucket. The salesperson who left in March still has the link. Ask to see what a salesperson at Store A can see about Store B, and watch the vendor's face. Access control is not a feature. It is the difference between a tool and a leak.

3. Can I get the logs? Event exports on your schedule, readable without asking. When something goes wrong, the first question from the customer, from counsel and from the FTC is what happened. A tool with no audit log cannot answer, and you cannot respond to what you cannot see. Logs are also how the AI gets better: when it answers badly, you trace where the answer came from and tune it. Logs you have to request are logs you do not have.

4. Who else touches it? A sub-processor list: every model, agent and API connection behind the tool, and you hear first when it changes.

5. What happens when we cancel? Contract ends, data ends, in writing. You will have sent this vendor customer data for years. Do they purge it, and how soon, or does it live on in some aggregate?

6. Show me, do not tell me. A SOC 2 report or a real architecture walkthrough, not a badge on a website. Plenty of vendors have the badge. Ask how.

A questionnaire is a vendor describing itself. Evidence is a vendor proving itself. I answer these questions as a vendor now. The good ones do not flinch.

When the vendor is two people and a laptop

Some of the best tools in this industry started that way. Vibe coded is not disqualifying. Unanswerable is. Three more questions:

1. Who reviews the code, and is it anyone other than the person who prompted it?
2. Where does it run, and who else has the root password?
3. What happens to my data when the founder goes on vacation, gets acquired, or quits?

Good small vendors love these questions. They are how a small vendor competes with a big one.

The tool nobody bought

The riskiest AI tool in your dealership is the one your team built on a personal account, on a Tuesday night, with a customer export. It works great. It has no vendor, no contract and no one to call.

Banning it does not work. People do not work harder when you ban a tool. They find the fastest way to get the job done and stop mentioning it. Sanctioning works: a paid AI workspace with real terms, a written list of what customer data can and cannot go in, and then one question to the team. Which AI tools are you already using that IT has never seen? The answer will surprise you.

The same rules for what you build

- **Name and measure.** Define the workflow and its success metric before you build. Speed, set rate, show rate. Pick one.
- **Log everything.** Every prompt, response and override, exportable.
- **Human in the loop.** Customer-facing actions need a person until the system has earned it.
- **Set end dates.** Every pilot gets a decision meeting. Still in pilot after six months means it already failed.

If you can trace the inputs, the logic and the overrides, you can trust it. If you cannot, you cannot.

Where to start

Five questions. The first no is your starting line.

1. Can I name every AI tool in my stores that touches customer data, including the ones nobody bought?
2. Do I have written data terms with each one, not just a login?
3. Could I pull a log of what any of them did last week, without calling the vendor?
4. Does anyone review a new tool before customer data goes into it?
5. Has my team told me what they built on their own?

Then thirty days.

- **Week one, inventory.** Every AI tool touching customer data, including the ones nobody bought.
- **Week two, ask.** The six questions to your top vendors. Write down who could not answer.
- **Week three, get the logs.** Event exports from every tool that passed. Prove you can read them.
- **Week four, decide.** Keep, kill or fix. Every tool gets an owner and an end date.

The six questions, on one page

1 **Where does my data go?**

Which model provider, which region, retained for how long, used for training or not.

2 **Who can see what?**

Named users, roles per store, multi-factor on every seat, access reviewed every quarter.

3 **Can I get the logs?**

Event exports on your schedule, readable without asking.

4 **Who else touches it?**

A sub-processor list, and you hear first when it changes.

5 **What happens when we cancel?**

Contract ends, data ends, in writing.

6 **Show me, do not tell me.**

A SOC 2 report or a real architecture walkthrough, not a badge on a website.

A questionnaire is a vendor describing itself. Evidence is a vendor proving itself.



Say hello.

Yuriy Demidko is Chief Technology & Product Officer at Clarivoy and speaks on leadership, momentum and AI that actually works. A self-taught engineer, he shipped 44 applications at Apple before becoming CIO of a major dealer group, where he built its AI in-house.

yuriy@yuriydemidko.com linkedin.com/in/yuriydemidko
yuriydemidko.com