

FTC Safeguards Rule Checklist for Dealerships

The nine elements every covered dealership needs under 16 CFR 314.4. Mark each one yes, no or not sure. If you can't put your hands on the proof, mark it no.

Dealership / rooftop

Completed by

Date

Required element	Yes	No	Not sure	Proof to keep, and where it lives
1 Name a Qualified Individual 314.4(a) One person runs the program and answers for it. An employee or an outside provider can hold the role.	☐	☐	☐	A signed, dated designation. _____
2 Put the risk assessment in writing 314.4(b) Where customer information lives, what could go wrong and the criteria you used to judge it.	☐	☐	☐	Each dated version and its criteria. _____
3 Build the safeguards 314.4(c) Eight specific technical controls. Work through them on page 2.	☐	☐	☐	The completed page 2. _____
4 Test and monitor 314.4(d) Continuous monitoring, or a penetration test every year plus a vulnerability assessment every six months.	☐	☐	☐	Test reports and the list of fixes. _____
5 Train your people 314.4(e) Security awareness training for everyone with a login. Security staff stay current on new threats.	☐	☐	☐	Sign-in sheets from each session. _____
6 Check your service providers 314.4(f) Choose vendors that can protect customer data, put security terms in the contract and reassess them.	☐	☐	☐	Vendor list, contracts and review dates. _____
7 Keep the program current 314.4(g) Update it after a test result, a new store, a DMS change or a new tool such as AI.	☐	☐	☐	Dated notes on what changed and why. _____
8 Write the incident response plan 314.4(h) Seven required parts, including roles, communications and how the weakness gets fixed. Practice it.	☐	☐	☐	The plan and notes from your last drill. _____
9 Report to the board 314.4(i) A written report from the Qualified Individual at least once a year, to the board or a senior officer.	☐	☐	☐	A copy of the report and who got it. _____

Fewer than 5,000 consumers in your records? Section 314.6 exempts you from the written risk assessment (2), the fixed testing schedule (4), the written incident response plan (8) and the annual board report (9). Everything else still applies.

Element 3 up close: the eight technical safeguards

Ask whoever manages your systems to show you each one working before you tick the box.

Technical safeguard, 314.4(c)	Yes	No	Not sure	Proof to keep, and where it lives
1 Access controls Each employee reaches only the customer information the job requires. No shared logins.	☐	☐	☐	A signed access review. _____
2 Data and device inventory What data you hold, which systems and devices hold it and who uses them.	☐	☐	☐	A current inventory. _____
3 Encryption Customer information encrypted where it's stored and in transit over outside networks.	☐	☐	☐	Encryption settings, system by system. _____
4 Secure applications Secure development for in-house tools. A security evaluation for software you bought.	☐	☐	☐	The evaluation for each application. _____
5 Multi-factor authentication MFA for anyone accessing your information systems, staff and vendors alike.	☐	☐	☐	MFA enrollment, user by user. _____
6 Secure disposal Customer information disposed of within two years of last use, unless you must keep it.	☐	☐	☐	Retention policy and a disposal log. _____
7 Change management A written procedure for changes to your network and systems.	☐	☐	☐	Change records with approvals. _____
8 Logging and monitoring Record what authorized users do. Watch for unauthorized access or tampering.	☐	☐	☐	Log retention and alert reviews. _____

Dates with hard numbers

Penetration test	Once a year, unless you run effective continuous monitoring.
Vulnerability assessment	Every six months, and after any material change to your systems.
Report to the board	In writing, at least once a year.
Customer data disposal	No later than two years after you last used it to serve that customer, unless a legal or business reason says keep it.
FTC breach notice	Within 30 days of discovering a breach of unencrypted information on 500 or more consumers.

Marked a few items no or not sure?

Bring this sheet to a complimentary IT and cybersecurity assessment.

heliontechnologies.com/it-assessment/

Source: 16 CFR Part 314, Standards for Safeguarding Customer Information, as of October 2026. This checklist is a self-assessment aid, not legal advice and not proof of compliance. © 2026 Helion Technologies.