FTC Safeguards Rule Compliance Checklist

For auto dealerships | Mapped to 16 CFR 314.4

- [ ] **1. Designate a Qualified Individual** `16 CFR 314.4(a)`
  Done looks like: One named senior person is accountable for the program, in writing.

- [ ] **2. Complete a written risk assessment** `16 CFR 314.4(b)`
  Done looks like: A dated document lists risks to customer data and how you rated them.

- [ ] **3. Implement safeguards and controls** `16 CFR 314.4(c)`
  Done looks like: Access controls, encryption of customer data, and multi-factor authentication are in place.

- [ ] **4. Test and monitor your controls** `16 CFR 314.4(d)`
  Done looks like: Continuous monitoring, or annual penetration testing plus periodic vulnerability scans.

- [ ] **5. Train every employee** `16 CFR 314.4(e)`
  Done looks like: All staff who touch customer data have current security-awareness training, records kept.

- [ ] **6. Oversee your service providers** `16 CFR 314.4(f)`
  Done looks like: DMS, CRM, and finance vendors are vetted and bound by contract to appropriate safeguards.

- [ ] **7. Evaluate and adjust the program** `16 CFR 314.4(g)`
  Done looks like: The program is updated when your systems, risks, or the Rule change.

- [ ] **8. Keep a written incident response plan** `16 CFR 314.4(h)`
  Done looks like: A written plan names who does what if customer data is compromised.

- [ ] **9. Report to leadership annually** `16 CFR 314.4(i)`
  Done looks like: A written report on the program goes to your board or dealer principal every year.

- [ ] **10. Be ready to notify on a breach** `16 CFR 314.4(j)`
  Done looks like: Report a qualifying event (unauthorized acquisition of unencrypted data of 500+ consumers) to the FTC within 30 days.

Hesitated on any item? That is a gap. A free gap assessment (for qualifying dealerships) turns this into a written report.
saferdealer.com/contact-us | (434) 317-6669