TRINITY CYBER

Helping Dealerships Meet the U.S. FTC Safeguards Rule

Solutions Brief

OCTOBER 2025

240.654.1451
info@trinitycyber.com

© Trinity Cyber Inc. 2025. All Rights Reserved | 16701 Melford Blvd #300, Bowie, MD 20715

TRINITY CYBER

Why FTC Compliance Matters to Dealerships

If you're writing or processing loans at your car dealership, you may not consider yourself a "financial institution" — but the U.S. Federal Trade Commission (FTC) does, even if you do not hold the loan yourself. FTC has classified auto dealers as a "non-banking financial institutions" subject to its revised Safeguards Rule cybersecurity regulation. Consider:

- Since May 2024, covered institutions must notify the FTC within 30 days of discovering a breach affecting more than 500 consumers. The FTC also published new auto-dealer-specific FAQs (Aug. 13, 2025) clarifying expectations.

- The revised FTC Safeguards Rule applies to auto dealers and other non-bank financial institutions because they process and store consumers' personal financial data. The Rulesets a national baseline for a "reasonable information security program."

  FTC has stated that the Revised Safeguards Rule "provides more concrete guidance for businesses." It mandates financial institutions establish and maintain a robust data security program, safeguarding sensitive customer information, including "non-public personal information." Among other things, the revised Safeguards Rule requires planning and action to address "reasonably foreseeable internal and external risks" – in other words, protection against data breaches, data leakage, phishing, and ransomware.

- Compliance pressure is real: 84% of consumers would not buy again from a dealer after a data compromise. NADA estimates many dealerships will spend >$100,000 to comply; 85% of dealerships say cybersecurity is a priority, yet 42% lack confidence in their program.

© Trinity Cyber Inc. 2025. All Rights Reserved

TRINITY CYBER

Trinity Cyber FCI

Full Content Inspection (FCI) opens, fully inspects, and **edits live session traffic inline** —removing malicious code **before** it reaches your environment, while letting legitimate business proceed. FCI operates continuously and at scale.

Dealership outcomes

- **Preempt ransomware**: strip payloads, neutralize exploit attempts, and blunt credential-harvesting—common dealership threats called out by the FTC focus on "reasonably foreseeable" risks.
- **Reduce incident scope & downtime** with automated, inline and real-time remediation.
- **Consolidate tools/cost** by replacing or augmenting legacy perimeter controls with a managed, preventive control.

© Trinity Cyber Inc. 2025. All Rights Reserved

TRINITY CYBER

We help you meet the Safeguards Rule

Rule element	Rule expectation	How FCI helps	Still needed
Risk-based program & foreseeable risks (§314.4(b), §314.4(c))	Written risk assessment; safeguards against **data breaches, leakage, phishing, ransomware**	**Continuously inspects** sessions and **removes malicious content**, giving you concrete evidence to inform your risk assessment and safeguards	Maintain a formal written risk assessment and governance process.
Monitoring & logging of authorized user activity (§314.4(c)(8))	Policies/controls to **detect unauthorized access or tampering**	**Remediates attacks in real time** (e.g., malware payload removal) and produces actionable evidence that supports documentation and evidence.	Maintain IR plan, roles, and tabletop exercises.
Continuous monitoring or testing (§314.4(d))	**Continuous monitoring** *or* periodic pen tests + vuln scans	**Continuous content-level monitoring and prevention** across inbound/outbound traffic, strengthening your "continuous monitoring" posture between scheduled tests.	Keep your pen-testing and vulnerability management program.
Incident response plan (§314.4(h))	Written IR plan with roles, comms, remediation, and documentation	**Contains attacks in real time** and produces actionable evidence that supports IR workflows, documentation, and post-incident improvements	Maintain IR plan, roles, and tabletop exercises.
FTC breach notification (§314.4(j))	Notify FTC **≤30 days** after discovery of incidents affecting **≥500 consumers**	FCI's deep session visibility accelerates **detection, scoping, and evidence collection**, helping you determine materiality and meet the FTC's timeline.	Legal/compliance process to file the notice on time.

Note on scope: **The Rule also requires controls outside FCI's remit—e.g.,** MFA**. Trinity Cyber integrates cleanly with your identity, encryption, networking, EDR, and governance stack.**

© Trinity Cyber Inc. 2025. All Rights Reserved

TRINITY CYBER

Why Trinity Cyber for dealerships

- **Prevention, not just detection.** FCI **edits** live traffic to remove threats—something legacy controls don't do—lowering false positives and operational friction.
- **Works with encrypted traffic.** With supported decryption, FCI brings **deep visibility and control** to both inbound and outbound flows—critical as dealership traffic is predominantly encrypted.
- **Operational simplicity.** Delivered as a **fully managed platform**, reducing tool sprawl and deployment burden that drive compliance costs.

Getting started

- Map your controls**: We'll align FCI to your control objectives and your dealer group's IR plan.**
- Deploy inline**: Stand up FCI for continuous inspection and real-time prevention across your enterprise and critical systems.**
- Prove it**: Use FCI reports/evidence to demonstrate how you're mitigating the** foreseeable risks **the FTC highlights for dealers.**

This document is informational and does not constitute legal advice. Dealerships remain responsible for interpreting and meeting all requirements of 16 CFR Part 314 and related FTC guidance.

© Trinity Cyber Inc. 2025. All Rights Reserved