

DONE-FOR-YOU SAFEGUARDS COMPLIANCE FOR AUTO DEALERSHIPS

Plus Protect Your Dealership from Class
Action Lawsuits and Cyber Insurance Risks

In October 2021, FTC updated the Safeguards Rule to address high-profile data breaches. Automotive dealers, among other financial institutions, must comply with the requirements to meet information security obligations.

NORTHROCK CYBERSECURITY OFFERS COMPLIANCE AS A SERVICE (CAAS) TO AUTOMOTIVE DEALERS

- Complete package covering all facets of the updated FTC Safeguards Rule; Physical and IT.
- Done-for-You compliance, including annual reports and risk assessments.
- Services of Chief Information Security Officer (vCISO) with 25+ years of experience in the automotive industry to validate compliance.

RISKS OF DELAYING SAFEGUARDS COMPLIANCE

1

AWAITING CONSUMER FRAUD LAWSUITS

Your Dealership Privacy Statement asserts that you will adhere to the Federal Safeguards requirements. It subjects you to class action lawsuits.

2

POSSIBLE CFPB INTERVENTION

Auto dealers delaying FTC Safeguards Compliance are at risk of CFPB intervention and banks refusing to cash their deals.

3

CYBER INSURANCE CLAIM DENIAL

Insurance companies deny claims due to "failure to follow" exclusions and negligence.

Our Done-for-You Safeguards Compliance program is backed by a \$1 million E&O policy.

**See detailed roadmap on reverse.*

FTC SAFEGUARDS COMPLIANCE PROGRAM: WHAT DO YOU GAIN?

DEVELOPMENT OF POLICIES & PROCEDURES

- Evaluation of current procedures and policies.
- Development and Approval of updated procedures and policies.
- Education and Training on Departmental Security Procedures.

VERIFICATION OF IT SECURITY CONTROLS

- Evaluation of existing security stack.
- Two-Factor Authentication for all logins.
- Encrypted data drives, mail services, and Security Awareness Training.

VENDOR COMPLIANCE TRACKING

- Gather contact information for vendors.
- Verify required vendor security controls.
- Periodically monitor vendors for compliance.

VULNERABILITY TESTING AND REMEDY PLAN

- Installation of testing device and network evaluation.
- Bi-yearly, vulnerability scans and reporting to IT, as required.
- Annual Penetration Testing and evaluation by security experts.
- Creating or revising Incident Response, Disaster Response, and Business Continuity Plans (IRP, DRP, BCP).
- Create and maintain Written Information Security Plan (WISP).

RISK ASSESSMENT AND ANNUAL REPORTS

- Performing periodic risk assessments, as required.
- Year-end vulnerability testing for final presentations.
- Preparation and presentation of Annual reports for Dealer Principal, GM, and other executives.

DON'T FALL VICTIM TO A DATA BREACH!

Take your dealership's security to the next level with our Safeguards Compliance Program

GET A QUOTE

GET IN TOUCH



(844) 570-9700



www.northrockcybersecurity.com