KATALYST

Schedule a Free FTC Compliance Call

FTC SAFEGUARDS

Compliance & Rule Checklist for Car Dealerships

The FTC Safeguards Rule is an integral part of their efforts to protect the security, confidentiality, and integrity of customer-sensitive information from cyberattacks, identity theft, and other types of fraud. Beginning June 9, 2023, the FTC Safeguards Rule will go live where all financial institutions, including “non-banking financial institutions” like auto dealerships, will be required to prove compliance.

On or before June 9th 2023, you must be compliant or you will run the risk of heavy financial penalties.This checklist will help you think through the 8 key areas you need to address to maintain compliance.

1. DESIGNATE A QUALIFIED INDIVIDUAL TO IMPLEMENT AND SUPERVISE YOUR COMPANY’S INFORMATION SECURITY PROGRAM

☐ This person can either be an in-house employee, or someone outside your company, such as an outside cyber security company. If you use an outside agency, make sure they also have a security program in place

2. CONDUCT A RISK ASSESSMENT

☐ A risk assessment is an overview of where your company’s potential vulnerabilities lie, and what data, technologies, and procedures need to be addressed. You may be exempt if you are responsible for less than 5000 consumer record.s

3. DESIGN AND IMPLEMENT SAFEGUARDS TO CONTROL THE RISKS IDENTIFIED THROUGH YOUR RISK ASSESSMENT

☐ **Implement and periodically review access controls.** In other words, take the time to understand which users have access to what data and other information.

☐ **Understand what your company’s data landscape looks like.** Routinely take a look at what information, systems, devices, and platforms you have, where they are kept, and how they are used

☐ **Encrypt customer information on your system and when it’s in transit.** If you have data that can’t be encrypted, use another security method at the recommendation of your designated “Qualified Individual”.

☐ **Assess your apps.** Implement procedures to assess the security of the apps your company uses, including both proprietary apps as well as third-party apps.

☐ **Implement multi-factor authentication for anyone accessing customer information on your system.** You will need to have at least two of the following authentication factors to be compliant: (There is an exception to this if your Qualified Individual has approved another form of secure access controls in writing.)

i) a knowledge factor (typically a password)
ii) a possession factor (ex, a token)
iii) an inherence factor (ex, biometric characteristics)

☐ **Dispose of customer information securely.** Securely dispose of customer information that you have not used to serve a customer in two years, unless you have a "legitimate business need or legal requirement" to keep the data, or if getting rid of the data is not possible, feasible, or practical.

☐ **Anticipate and evaluate changes to your information system or network.** Be ready to adjust and scale your safeguards as needed and to build your information security program with adjustments in mind.

☐ **Maintain a log of authorized users' activity and keep an eye out for unauthorized access.** Implement procedures to monitor when authorized users are accessing customer information on your system and to detect unauthorized access attempts.

4. REGULARLY MONITOR AND TEST EFFECTIVENESS OF YOUR SAFEGUARDS

☐ **Conduct a penetration test every year**, or any time your system undergoes a change or otherwise may encounter new vulnerabilities.

☐ **Conduct regular vulnerability scans every six months**. Alternatively, you can implement continuous monitoring of your information systems.

5. TRAIN YOUR STAFF

☐ **Ensure our staff, especially non IT staff, understand the basics of cyber security** and cyber attack avoidance. A reputable cyber security company can assist with training them.

6. MONITOR YOUR SERVICE PROVIDERS

☐ **Make it clear and document it.** Lay out expectations in your contracts with your service providers and develop ways to monitor and regularly assess their security strategies.

7. KEEP YOUR INFORMATION SECURITY PROGRAM CURRENT

☐ Update your security program based on new discoveries and threats, or changes in your business and keep your program ready to change when needed.

8. CREATE A WRITTEN INCIDENT RESPONSE PLAN

☐ Keep a detailed plan of exactly what you will do in the event of a cyber attack or other emergency that puts your data at risk. It should be updated whenever you change your technology or hire new staff.

Your written plan needs to cover:

- ☐ Goals of the plan
- ☐ Internal processes your company will activate in response to a security event
- ☐ Clear roles, responsibilities, and levels of decision-making authority within your company
- ☐ Communications and information sharing both inside and outside your company
- ☐ A process to fix any identified weaknesses in your systems and controls
- ☐ Procedures for documenting and reporting security events and your company's response
- ☐ A post mortem of what happened in the event of an incident, with a revision of your incident response plan and information security program based on what you learned.

REQUIRE YOUR QUALIFIED INDIVIDUAL TO REPORT TO BOARD OF DIRECTORS

☐ They will need to submit a written report to your board of directors or a "senior officer responsible for your information security program" every year.

The report needs to include:

- ☐ Risk assessment
- ☐ Risk management and control decisions
- ☐ Service provider arrangements
- ☐ Test results
- ☐ Any new security events (attempted attacks) and what the response was
- ☐ Any recommendations for changes to the security program

Looking for help in getting ready for the June 9 FTC compliance deadline?

Schedule a call with the Katalyst team