



IT Solutions

FTC Safeguards Rule: A Guide for Car Dealerships

CONNECTIONS THAT MOVE YOU


 IT Solutions / Digital Sales / CRM / F&I / DMS / Fixed Operations / Intelligence



Table of Contents

03 WHY IS
CYBERSECURITY ESSENTIAL?
Understand the risks of staying unprotected.

05 WHAT ARE THE
FTC SAFEGUARDS?
A review of the regulation and its requirements.

06 WHY ARE THESE
SAFEGUARDS IMPORTANT?
Learn about the impact of the regulations
and the price of noncompliance.

07 DETAILS OF THE
FTC SAFEGUARDS
A closer look at the specific requirements for dealers.

09 FIVE STEPS TO
PREPARE FOR COMPLIANCE
A step-by-step breakdown of how to prepare
for the December deadline.

10 KEY TAKEAWAYS
Things you need to know moving forward.



Why Is Cybersecurity Essential?

From ransomware to data breaches, dealerships are under attack at unprecedented levels and protecting your data has never been more important.

The risk of IT-related business interruptions or reputational damage has an enormous potential impact. It's time to assess, reassess and improve cybersecurity at your dealership.

Today's Dealership Security Threat Landscape

36%

Of data breaches are phishing attacks

Source: Verizon data breach report 2021

70%

Of dealerships' antivirus is not current

Source: Total Dealer Compliance

11 seconds

The frequency with which ransomware is expected to attack a business

Source: Cybersecurity Ventures



Do Any of These Statements Apply to Your Dealership?

- 1 You don't have preventative and protective cybersecurity in place right now
- 2 You don't have a qualified individual to oversee your dealership's data security
- 3 You don't have multifactor authentication
- 4 You haven't conducted a risk assessment within the past 12 months
- 5 You aren't reviewing risks associated with your third-party partners and vendors
- 6 You haven't conducted a data and systems inventory check
- 7 You don't have an incident plan in place outlining your response to a cyberattack or loss of service
- 8 You don't have 24/7/365 security monitoring in place to detect cyberthreats and malicious events

If any of these apply, you are more likely to be the victim of a costly cyberattack.

Top Dealership Threats



Ransomware



Malware



DDoS



Social Engineering



Phishing

Lost Revenue

16 days

Average length of downtime due to ransomware

Source: Coveware Ransomware Marketplace report

Cost of Inaction

\$220,298

Average payout to thieves in a ransomware attack

Source: CyberScoop 2021

Lost Customers

84%

Of consumers said they would not go back to buy another vehicle after their data had been compromised

Source: Total Dealer Compliance



What Are the FTC Safeguards?

The Federal Trade Commission (FTC) announced an update to the Standards for Safeguarding Customer Information under the Gramm-Leach-Bliley Act (GLBA) on October 27, 2021. This GLBA change went into effect December 9, 2021, with full compliance required by December 9, 2022.

These amendments were enacted to help keep customer financial information secure from cyberattacks and security breaches, and to address recent high-profile data breaches.



Calls out motor vehicle dealers, mortgage brokers and payday lenders



Institutions must develop, implement and maintain a comprehensive security system to keep their customers' information safe



FTC strengthens security safeguards for consumer financial information following widespread data breaches



Why Are These Safeguards Important?

The Safeguards Rule establishes prescriptive information security program standards. Dealers must appoint a qualified individual — a Chief Information Security Officer (CISO) — to supervise data security and adherence to these new standards. Not only will these standards have a significant influence on dealership operations, they carry with them monetary penalties if dealers are not in compliance by the deadline. This new revision applies to all dealers and requires documented risk assessment, an incident response plan and a yearly report to a board of directors. Dealerships that have gathered data on less than 5,000 customers are exempt from some of the new obligations.

The FTC Safeguards Rule Covers a Broad Scope, Including:

- 1 Risk assessment
- 2 Information disposal procedures
- 3 Access controls
- 4 Change management
- 5 Data inventory and classification
- 6 Testing
- 7 Encryption
- 8 Incident response
- 9 Secure development practices
- 10 Employee training
- 11 Authentication
- 12 Vendor oversight



Details of FTC Safeguards

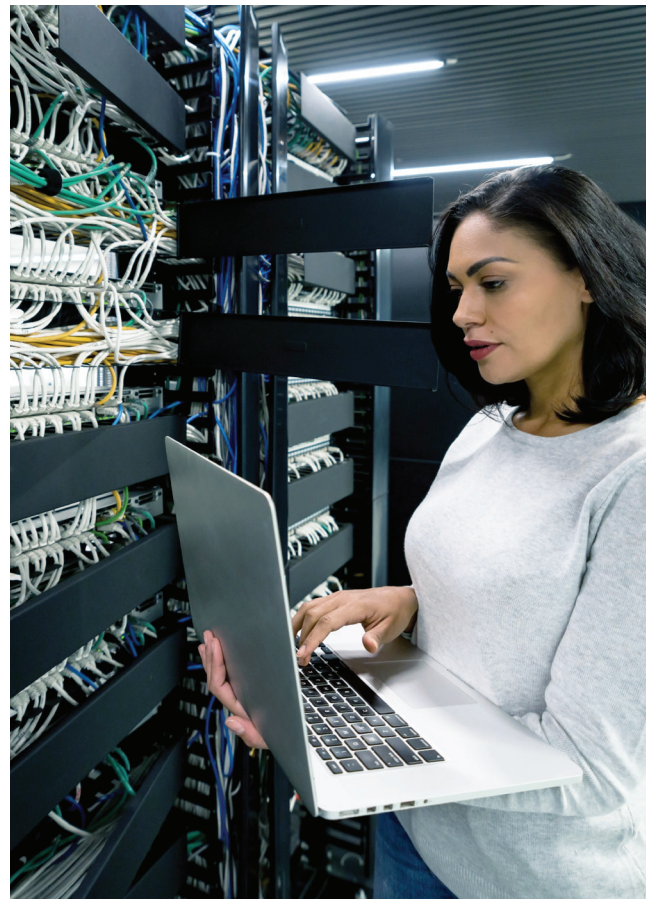
In General, the FTC Dealer Requirements Entail:

- Reviewing current systems and the information they maintain
- Developing a written plan demonstrating methods to protect consumer data
- Identifying a qualified individual to oversee data security
- Notifying consumers in the event of any unauthorized person gaining access to data or the system

Terms and related examples are made specific in this updated regulation, rather than referencing them through a related FTC rule.

Below are highlights of this change in greater detail:

- **Detailed requirements for the development and implementation of a written information security program**
These include risk assessment, system access controls, authentication and encryption, mechanisms to ensure effective employee training and oversight of service providers.
- **Mandatory qualified individual responsible for the information security program**
They must submit periodic reports to boards of directors or governing bodies to provide senior management with data security status.
- **Exempts entities collecting information on fewer than 5,000 consumers**
Written risk assessments, incident response plan and annual reporting to a board of directors are not required.
- **Expands the definition of financial institution to include finders**
These third parties bring together buyers and sellers of a product or service. Dealerships are responsible for ensuring any vendors with whom they share information are also in compliance with the rule.



16 Updates to FTC Safeguard Rules

- 1 A qualified individual to oversee cybersecurity accountability
- 2 Information security program to be based on a written risk assessment
- 3 Data and systems inventory
- 4 Data encryption at rest and in transit
- 5 Adoption of secure development practices
- 6 Multifactor authentication
- 7 Required audit trails
- 8 Secure disposal procedures
- 9 Adoption of procedures for change management
- 10 Unauthorized activity monitoring
- 11 Penetration testing and vulnerability assessments
- 12 Employee training and security updates
- 13 Periodic assessment of service providers
- 14 Incident response plan
- 15 Written CISO report
- 16 Implementation of access controls



Five Steps To Prepare for Compliance

We Recommend These as a Good Starting Point

- 1 **Appoint a dedicated security person within the dealership to be responsible for all compliance measures**
 - Keep accurate documentation
 - Report back to senior leadership
- 2 **Inventory the network and all security controls**
 - Identify relevant data, personnel, devices, systems and facilities
 - Ensure access controls are in place for information systems
- 3 **Get a risk assessment**
 - Draft a written risk assessment containing and addressing specific additional issues/areas of risk
 - Use this risk assessment as the basis for your written security program
- 4 **Ensure your paperwork is up to date**
 - Review plans for information security, incident response and risk assessment
 - Amend as needed for compliance
- 5 **Implement required security controls**
 - Multifactor authentication
 - Cybersecurity awareness training
 - Security event monitoring and detection
 - Encryption of customer data

How to Get Started

CDK offers a free cybersecurity and network evaluation to help dealers:



Assess their strengths and gaps in their current environment



Outline recommendations for current and future improvements



Estimate scope and costs for next steps

We also encourage dealers to review FTC documentation outlining key requirements.

Read the **FTC Safeguards Rule: What Your Business Needs to Know** to learn more about the important aspects that dealers need to know.



Key Takeaways

- Every dealer is impacted, regardless of OEM (U.S. only)
- Less than a year remains for compliance — the clock started on December 9, 2021
- Some requirements have a 30-day compliance window
- Significant changes for dealership operations
- Dealers must designate a qualified individual to oversee data security

CDK Global has solutions for you today and is constantly working to provide you with state-of-the-art technology and even more infrastructure solutions.

Get started today with a **Cybersecurity Evaluation**.

Disclaimer: This document is not intended to be used as legal advice. The Safeguards Rule's requirements and the unique conditions of each dealership are complicated, and dealers should not just follow the sample information. Furthermore, this e-book only covers the FTC Safeguards Rule; it does not cover any state or local laws that may impose extra requirements that you may be subject to by contract. All required policies and procedures specific to your dealership should be written and implemented, and they should be thoroughly evaluated by expert legal counsel.

CDK GLOBAL[®]

Learn more at CDKGlobal.com