

NEW FTC SAFEGUARDS RULE | ARE YOU PREPARED?

The Federal Trade Commission (FTC) has finalized changes to the Standards for Safeguarding Customer Information rule (Safeguards Rule) under the Gramm-Leach-Bliley Act (GLBA). The updated Safeguards Rule amends the FTC's 2003 Safeguards Rule and requires financial institutions (which includes Dealers) to strengthen their data security safeguards to protect customer financial information. **Compliance with the updated Safeguards Rule is required by December 9, 2022.**

The updated Safeguards Rule now includes specific criteria for what safeguards financial institutions must implement as part of their information security program. Previously, similar rules provided only general guidance and not specific requirements. **Among other requirements, the updated Safeguards Rule mandates the following:**

- **Designation of Qualified Individual:**

Designate a qualified individual to be responsible for the information security program.

- **Written Information Security Program:**

Establish a comprehensive written information security program, including designating a qualified individual for overseeing and implementing the program.

- **Risk Assessments**

Undertake risk assessments and implement safeguards to address identified risks. Assessments must be in writing and include criteria for evaluating and identifying security risks, as well as ways to mitigate or accept those risks. Risk assessments must be performed periodically to reassess the reasonably foreseeable risks to the security of customer information.

- **Penetration Tests and Vulnerability Assessments:**

Annual penetration tests of information systems. Vulnerability assessments, including any system scans or reviews of information systems, must be completed every 6 months.

- **Encryption of Customer Information at Rest and in Transit:**

Encrypt all customer information, both in transit over external networks and at rest.

- **Service Provider Oversight:**

Take reasonable steps to select and retain third-party service providers that maintain appropriate safeguards for customer information and periodically assess service providers to ensure compliance.

- **Additional Training Requirements:**

Update the training for employees based upon risk assessments and/or changes in practices and verify that training requirements have been met.

- **Multifactor Authentication:**

Implement multifactor authentication for individuals accessing networks that contain customer information. Authentication measures may include (1) knowledge factors (a password); (2) possession factors (a token); or (3) inherence factors (biometric characteristics).

- **Logging and Disposal of Customer Information:**

Develop, implement, and maintain procedures for the secure disposal of customer information no later than 2 years after the last date the information was used, unless otherwise required to retain the information longer, and implement policies, procedures and controls designed to monitor and log the activity of unauthorized users and detect unauthorized access, use or tampering with customer information.

- **Reports to Board of Directors:**

The qualified individual must provide written reports at least annually to boards of directors or governing bodies on the financial institution's information security program. Including information on the overall status of the information security program and the financial institution's compliance, and material matters related to the information security program (such as risk assessments and recommended updates to the program).

Dealers Must Comply by **December 9, 2022**

OUR LMS PREPARES YOU 

CONTACT US TO TODAY 866.273.3848 | sales@700credit.com

700Credit is the largest provider of credit, compliance, and soft pull solutions for automotive retailers.



LEARNING MANAGEMENT SYSTEM

Get the required training your dealership needs to adapt to these new rules and avoid costly fines

To further our efforts in providing the best compliance and risk mitigation services to our clients, we are pleased to introduce our new web-based, self-paced Compliance platform which will provide the required training your dealership needs to remain compliant with every transaction and avoid costly fines.



LEARN MORE AT:
700credit.com/compliance-training

Can You Afford to Pay Penalties for Non-Compliance?

Dealers are fined millions of dollars every year for not following the proper government regulations around the accessing and handling of customer's sensitive credit data. As the largest reseller of credit reports from all three bureaus – Experian, Equifax and TransUnion – 700Credit has always strived to provide a comprehensive and automated compliance solutions to keep you compliant with every credit report pulled.

This Compliance platform meets the guidelines set forth by the 3 major credit bureaus on the rules and regulations all business must follow when pulling a credit report and is required for every dealership that uses our credit report solution.

For more information, visit our website:
www.700credit.com.

Course Name	Course Description
Adverse Action Rule	This course helps to identify when information in a consumer report results in an adverse action and requires a proper notice to be provided to the customer as required by the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA).
IRS Rule 8300	Helps identify which transactions are considered cash transactions that require submission of an IRS Form 8300.
Paper Flow	Reviews the importance and necessity of properly handling and retaining paperwork as required by GLB and the FTC Safeguards and Disposal Rules.
Privacy	The goal is to provide you with enough information so that you will know how to protect customers' non-public information (NPI) as required by the Gramm-Leach-Bliley Act (GLB).
Red Flag Rule	Helps dealership employees identify the red flags of identity theft and fraud, and to help prevent fraudulent conduct.
Risk Based Pricing Notices	Describes the risk-based pricing rule and best practices you need to follow at your dealership to comply.
UDAAP	Provides information on avoiding acts and practices that can be unfair, deceptive, or abusive – and illegal, or better known as UDAAP.
OFAC	Help your dealership comply with the Office of Foreign Asset Controls (OFAC) requirement that car dealers check customer names against a database of known dangerous organizations and individuals.

CONTACT US TO TODAY 866.273.3848 | sales@700credit.com

700Credit is the largest provider of credit, compliance, and soft pull solutions for automotive retailers.

