FTC Safeguards Rule Amendments Playbook

What are they, and how Reynolds can help.

Retail Management System

Reynolds & Reynolds®

This document is not intended and does not constitute legal advice or recommendations. You are responsible for compliance with applicable laws and regulations, and you should seek your own legal advice and counsel with regard to compliance with the legal obligations described in this document.

In October 2021, the Federal Trade Commission (FTC) announced amendments to the Safeguards Rule. These amendments impact the security measures businesses that are considered non-banking financial institutions should implement for protecting consumer information. The amendments to the rule will take effect on December 9, 2022.

In this booklet, we'll provide answers to frequently asked questions around the Safeguards Rule, its impact on dealerships, and what Reynolds is doing in light of these amendments.

WHAT IS THE GLB ACT?

The Gramm-Leach-Bliley Act, otherwise known as the GLB Act, is a federal law enacted in the United States on November 12, 1999. Among other things, this law requires financial institutions to ensure the security and confidentiality of personal information they collect from their consumers. Under the act, dealerships are considered a financial institution.

For more information, visit:
https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

WHAT IS THE SAFEGUARDS RULE?

The Safeguards Rule took effect in 2003 with amendments being made in the fall of 2021. The Rule lays out specific ways in which financial institutions, including dealerships, are required to protect customer information.

As part of the Rule, all covered companies must have a written information security program describing your plan to protect customer information.

The Rule lays out nine elements required to be part of your plan:

1. Designate a qualified individual to implement and supervise your company's information security program
2. Conduct a risk assessment
3. Design and implement safeguards to control the risks identified through your risk assessment
   a. Implement and periodically review access controls
   b. Know the data you have and where it is stored
   c. Encrypt customer information at rest and in transit
   d. Access your applications and evaluate their security
   e. Implement multi-factor authentication for accessing customer information on your system
   f. Dispose of customer information securely
   g. Anticipate and evaluate changes to your information system or network
   h. Maintain a log of authorized users' activity and monitor unauthorized access
4. Regularly monitor and test the effectiveness of your safeguards
5. Train your staff on security awareness measures
6. Monitor your service providers
7. Keep your information security program current through regular monitoring
8. Create a written incident response plan
9. Require your qualified individual to report regularly to your Board of Directors or senior officers

For more details on the above requirements, please visit:
https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

WHAT IS INCLUDED IN THE AMENDMENTS THAT HAVE A COMPLIANCE DEADLINE OF 12/9/22?

The amendments to the Safeguards Rule provide specificity to what must be implemented.

1. Qualified Individual must report in writing to your Board of Directors annually (or senior officers if you do not have a Board of Directors)
2. Conduct periodic risk assessments
   a. Must be written and include criteria used for evaluation
3. Implement and review access controls (who has access to what)
4. Document an inventory of your data
5. Encrypt data at rest and in transit
6. Document a process to evaluate vendors' security
7. Enable Multi-Factor Authentication (MFA) when accessing consumer information
8. Securely dispose of customer information within two years
   a. The only exceptions: if you have a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible because of the way the information is maintained.
9. Document change management processes for your network
10. Monitor and document who is accessing what information and when
11. Monitor and test the effectiveness of your security plan
12. Train your staff on your plan
13. Monitor service providers and their data security plans
14. Your plan must provide flexibility to be updated
15. Written incident response plan

For more information, please visit:
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4

WHAT CAN REYNOLDS HELP WITH?

Implement and review access controls (who has access to what)

Safeguards Rule:

"Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against unauthorized acquisition of customer information..."

How can you do this today?

> Reynolds software allows administrators to grant and remove user access and provides reporting that details what items users can access.

> If you do not know how to grant / remove access or generate access reports, please contact the following:

ERA-IGNITE Technical Assistance Center: **800.767.0080**

POWER Support Center: **888.999.6348**

WHAT CAN REYNOLDS HELP WITH?

Monitor and document who is accessing what information and when

Safeguards Rule:

"Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."

How can you do this today?

> Reynolds Interface Dashboard allows you to see what information is being sent outside of the system and where it is going.

> Reynolds Certified Interface program tracks data changes from third-party vendors to provide tools to help identify data corruption with the ability to provide support if a data incident occurs.

> Reynolds is in the process of building log screens and reporting showing data sets a user accesses within the system and activities that were made to view, edit, or delete customer information. This is expected to release in the fall of 2022.

WHAT CAN REYNOLDS HELP WITH?

Enable Multi-Factor Authentication (MFA) when accessing consumer information

Safeguards Rule:

"Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access systems."

How can you do this today?

> Reynolds is in the process of building MFA functionality into our systems. ERA-IGNITE and POWER both have dlrSecured Mass Enrollment screens currently available so users can begin preparing for the release of MFA functionality. Users can view details in the ERA-IGNITE 31.50 and POWER 38.500 Program News documents.

> General release of MFA functionality is expected to start 10/1/22.

WHAT CAN REYNOLDS HELP WITH?

Securely dispose of customer information within two years

Safeguards Rule:

"Develop, implement and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained."

How can you do this today?

> Reynolds software allows users to delete or securely mask customer information.

> If you do not know how to delete customer information, please contact the following:

ERA-IGNITE Technical Assistance Center: **800.767.0080**

POWER Support Center: **888.999.6348**

WHAT CAN REYNOLDS HELP WITH?

Encrypt data at rest and in transit

Safeguards Rule:

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

How can you do this today?

> Data in the Reynolds system is stored in an encrypted manner. Customer information is also encrypted when sent outside of the system.

> Reynolds Certified Interface program allows you to send data outside the system securely using real-time, bi-directional, custom-built interfaces for each certified third party.

WHAT CAN REYNOLDS HELP WITH?

Monitor and test the effectiveness of your security plan

Safeguards Rule:

"Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems."

How can you do this today?

> Reynolds offers several IT and cybersecurity solutions that assist you in meeting these requirements through Proton Dealership IT.

WHAT CAN REYNOLDS HELP WITH?

Train your staff on your plan

Safeguards Rule:

"Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment..."

How can you do this today?

> Reynolds is in the process of developing dealership-specific security training courses.

> The security training courses are expected to be available by the fall of 2022.

RELATED RESOURCES

FTC Safeguards Rule: What Your Business Needs to Know

NADA Amended Final Safeguards Rule FAQ

Automotive Endpoint Defender

Managed Firewall and other Networking solutions

Proton Dealership IT

For more information about Reynolds IT and cyber security offerings or safeguards questions, please contact the following:

Reynolds and Reynolds:
info@reyrey.com | 800.767.7879

Proton Dealership IT:
sales@protontechs.com | 800.278.0034

Reynolds & Reynolds®