nuspire

FTC Safeguards Rule
Dealership Guide

Recent amendments to the FTC Safeguards Rule introduce more comprehensive controls and added complexity to dealers' security compliance processes. This guide is designed to help you understand and address the new amendments to ensure you're in compliance.

Table of Contents

FTC Safeguards Rule:

What Auto Dealers Need to Know

The FTC's Safeguards Rule has been around for nearly 20 years, requiring financial institutions (including automotive dealers) to comply with specific security guidelines to protect customer data. However, recent amendments to the rule introduce more comprehensive controls and added complexity to dealers' security compliance processes.

In fact, since the new requirements are extensive and complicated, many dealers will likely incur significant costs to comply.

In this guide, we break down the essentials and explain actions you can take to set yourself up for successful compliance by December 9, 2022.

What is the Safeguards Rule?

The Safeguards Rule – which originally went into effect in 2003 under the federal Gramm-Leach-Bliley Act (GLBA) – requires financial institutions (including automotive dealers) to put in place measures that keep customer information secure. The rule classifies auto dealers as financial institutions because they offer financing agreements.

Note that this Safeguards Rule is distinct from the Privacy Rule under the GLBA. The Privacy Rule addresses how institutions and dealers share information about consumers who obtain or apply for credit or lease products from them. The Safeguards Rule addresses how these entities must protect that consumer information.

What does the updated rule require?

On October 27, 2021, the FTC issued its final amendments to the rule to address "recent high-profile data breaches." The rule amendments include a substantial number of new and expanded procedural, technical and personnel requirements that financial institutions, including automotive dealers, must satisfy to meet their information security obligations.

At a high level, the rule is not as flexible as it used to be around data security. Now it mandates that all financial institutions (including dealers) must satisfy a list of requirements regardless of their size, systems, or the types or scope of data they maintain.

A Few Key Changes

- Adds detailed requirements for the **development and implementation of a written information security program** mandated under the existing rule. These include requirements for risk assessment, system access controls, authentication and encryption, and mechanisms to ensure effective employee training and oversight of service providers.
- Requires institutions appoint a **"qualified individual"** to be responsible for the information security program. That person must submit periodic reports to boards of directors or governing bodies so senior management has better awareness of their data security safeguards.
- Expands the definition of "financial institution" to include **"finders,"** which are companies that bring together buyers and sellers of a product or service. This means that the dealerships are responsible for ensuring that the vendors they share information with also meet the requirements of the rule.
- Defines terms and provides related examples in the rule itself instead of incorporating them by reference from a related FTC rule.

Under the rule, financial institutions must specifically:

> **"Develop, implement and maintain a [written] comprehensive information security program" that "contains administrative, technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities and the sensitivity of any customer information at issue."**

Simply put, they must write a document explaining the steps they take to protect the customer data on their systems.

How Does Nuspire Help?

1. All dealerships and retailers have access to security consultants to help answer questions around the rule and provide guidance on what steps to take for their unique environments.
2. Utilizing managed detection and response (MDR) and endpoint detection and response (EDR) solutions, Nuspire monitors retailer environments 24x7 to detect and remediate security events on the client's behalf. This helps to meet a significant portion of the FTC Safeguards Rule:
   - Continuous monitoring of security events and user activity
   - Nuspire's SLAs will become a significant portion of the required written incident response plan for the client, detailing how we respond to different levels of security events. In addition, our teams become an extension of the client's team for incident response.
   - Nuspire retains the logs of these events for 400 days, surpassing the requirement for a year of log storage – at no additional cost to the client.
3. Nuspire has partnered with NADA-Affinity solution providers to help meet the rest of the requirements including:
   - Risk assessments
   - Auditing the client's vendors to ensure they are compliant with the rule, saving the client the headache of having to do it themselves
   - Providing guidance and templates for the written requirements of the rule
   - Providing cybersecurity awareness training

Nuspire's OEM partnerships enable our clients to take advantage of these enterprise grade solutions, at a fraction of what it would cost them to do deploy and manage the solutions on their own.

Next Steps:

What To Do Now

The FTC's amended Safeguards Rule can be overwhelming to understand. Here are some actions you can take right now to set yourself up for success in complying with the rule.

Contact a security consultant today to review the "Get Compliant Checklist" and build a plan.

Your consultant will be able to provide guidance on the following:

- Leveraging compliance partners to complete a risk assessment and begin an asset inventory.
- Implementing mandatory controls, including continuous monitoring, cybersecurity awareness training and more.
- Designating a qualified individual to maintain and report on the written information security program.
- Documenting a written information security program and an incident response plan.
- Evaluating your vendors and ensuring they are compliant.

FTC Safeguards Get Compliant Checklist

NEXT STEPS	CLIENT	NUSPIRE + ACCELERATE 2 COMPLIANCE
GET YOUR PLAN IN MOTION		
Speak to a consultant to start building your Get Compliant Plan		X
Appoint a single qualified individual to oversee the program	X	
Conduct risk assessments on infosec infrastructure and existing safeguards		X
IMPLEMENT MANDATORY CONTROLS		
Access controls and encryption on all customer information	X	
Multi-factor authentication		
Continuous monitoring and log retention		X
Cybersecurity awareness training		X
REGULARLY TEST OR AUDIT THE EFFECTIVES OF CONTROLS		
Continuous monitoring of events and user activity OR Annual penetration testing and bi-annual vulnerability scans		X
OVERSEE YOUR VENDORS		
Evaluate vendors to ensure their compliance with the rule		X
DOCUMENT YOUR WRITTEN SECURITY PROGRAM AND REPORT ANNUALLY TO SENIOR LEADERSHIP		
Written system inventory	X	X
Create a written information security program and a written incident response plan	X	X

Frequently Asked Questions

Which requirements are unique to auto dealers?

Parts of the amendments are specific to automotive dealers:

- In addition to developing their own safeguards, dealers must ensure their affiliates and service providers safeguard the customer information in their care.
- To do this, dealers must audit their vendors for compliance.
- If a dealer fails to ensure any vendor complies, they may be penalized or fined in the event of an audit or security breach.

What are the key deadlines?

Within 30 days of the October 27, 2021 publication, financial institutions and dealers needed to comply with the following sections of the amended rule (many of which were existing requirements):

- 314.4(b)(2)—Additional periodic risk assessments.
- 314.4(d)(1)—Regularly test or monitor effectiveness of the safeguards key controls, systems, or procedures
- 314.4(f)(1) and (2)—Overseeing service providers by: (1) taking reasonable steps to select and retain, and (2) requiring specific contract terms.
- 314.4(g)—Evaluate and adjust your information security program considering the results of the testing and monitoring required by paragraph (d).

By December 9, 2022, financial institutions and dealers must comply with all remaining requirements of the rule and amendments as outlined on the **Code of Federal Regulations** site.

Why is the FTC changing the rule?

The FTC proposed amendments to the current rule is in response to pressure to address “recent high-profile data breaches.” It includes a series of new technical requirements.

Frequently Asked Questions

What has changed?

Some of the specific changes are listed in the Appendix below, but at a high level, the amended rule modifies the current flexible approach to data security by mandating a list of requirements that all financial institutions (including dealers) must meet, regardless of their size, systems, or the types or scope of data they maintain.

This means that for a dealer to comply with the amended rule, the dealer must take each of the steps and actions outlined in the amended rule—without any determination as to the security benefit of those actions.

In addition, dealers must ensure that any of their vendors that access any customer data must also comply with these same requirements, and dealers must audit them for compliance. If a dealer is unable to do so, the FTC has said that the dealer may no longer engage that vendor.

Are there any exceptions?

There is an exception to many of the new requirements within the amended rule for any entity that maintains 5,000 or fewer customer records. Few, if any, dealers will be able to take advantage of this exception. However, dealers should consult with their vendors and professional advisors concerning this exception as well as the other aspects of the new requirements.

Will this be expensive for dealers?

There is no clear answer to that question, but the new requirements are certainly extensive, complicated and for many dealers, will add significant costs.

What are the penalties for not complying?

Penalties may include long-term consent decrees with your companies (and sometimes your executives), extensive injunctive relief and potential fines up to $46,517 per violation.

Are all OEMs included?

There is no exception—and never has been—for your relationship with your OEM. Any programs you participate in, or services you obtain from your OEM, must comply with the requirements of the Safeguards Rule to the extent customer data is shared.

I have been contacted by a vendor claiming to be able to “get my dealership compliant” with the FTC Safeguards Rule - are they legitimate?

Many companies have been claiming to be a “one-stop-shop” to get to compliance, which sounds appealing; however, given the wide scope of the requirements, there are few, if any, vendors who have the capabilities to cover every control.

For a business to meet all of the required controls, it will likely need to work with a few different vendors, including:

- Vendors for risk assessments
- Providers such as Nuspire for managed security services and incident response
- Existing third-party providers for implementing mandatory technologies such as multi-factor authentication or securing existing infrastructure and software

A vendor is suggesting that we use penetration testing rather than continuous threat monitoring. What do you suggest?

Vulnerability scans and penetration tests versus continuous security management and monitoring are different types of solutions that produce very different outcomes, and both are recommended functions of a mature security program. Our recommendation is always to **do both** because vulnerability analysis and reporting doesn't ensure that remediation activities will follow.

Regardless of what we would recommend as a part of a mature security program, the FTC Safeguards Rule allows for one or the other. A combination of managed security services including managed detection and response (MDR) and robust endpoint detection and response (EDR) not only satisfies this requirement, but also satisfies many other requirements, including the infrastructure guidelines published by the OEMs and many cybersecurity insurance requirements.

> **"Finding that you left the back door unlocked before you go to bed isn't nearly as effective from a risk management standpoint as locking the door in the first place."**
> — Mike Pedrick, VP of Cybersecurity Consulting, Nuspire

Appendix

The following is a brief overview of the primary new requirements dealers must undertake pursuant to the Amended Safeguards Rule.

Appointment of a "Qualified Employee"

- Currently, dealers must designate an "employee or employees to coordinate your information security program."
- The Amended Rule instead requires dealers to designate "a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program."
- The proposal initially required the appointment of a Chief Information Security Officer (CISO). This is one area where the FTC made an important change, noting that the "qualified" employee does not need to be a CISO.

Requirement to Undertake a Written "Risk Assessment"

- The Amended Rule requires that a new written document—a "risk assessment"—be drafted, and that it must contain and address certain areas of risk at the financial institution.
- The rule currently requires dealers to undertake a risk assessment. What has changed is that this risk assessment must now be in writing, and it must address specific additional issues and areas of risk. The Amended Rule also requires additional periodically performed risk assessments.

Implementation of "Access Controls"

- The Amended Rule requires dealers to "place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of customer information and to periodically review such access controls."

Undertake a Required Data and Systems Inventory

- The Amended Rule requires dealers to "Identify and manage the data, personnel, devices, systems, and facilities that enable [the financial institution] to achieve business purposes in accordance with their relative importance to business objectives and [the financial institution's] risk strategy."

Data Encryption Requirement

- The Amended Rule requires dealers to "encrypt all customer information, both in transit over external networks and at rest."
- This requirement also extends to all dealer vendors and others with access to dealership customer data.

Appendix Cont.

Requirement to Adopt Secure Development Practices and Assess Externally Developed Applications

- The Amended Rule requires dealers to "Adopt secure development practices for in-house developed applications utilized" for "transmitting, accessing, or storing customer information" and requires "procedures for evaluating, assessing, or testing the security of externally developed applications [financial institutions] utilize to transmit, access, or store customer information."

Multi-Factor Authentication

- The Amended Rule requires dealers to "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 controls."
- Again, this requirement applies equally to service providers that house or access dealership data or systems.

Systems Monitoring and Logging

- The Amended Rule requires dealers to "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."

Development of Secure Data Disposal Procedures

- The Amended Rule requires dealers to "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."

Required Change Management Procedures

- The Amended Rule requires dealers to "to adopt procedures for change management" that "govern the addition, removal, or modification of elements of an information system."

Appendix Cont.

Required Unauthorized Activity Monitoring

- The Amended Rule requires dealers to implement policies and procedures designed "to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."

Required Intrusion Detection and Vulnerability Testing

- The Amended Rule requires dealers to "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."

Series of New Requirements to Ensure that Personnel Are Able to Enact the Information Security Program

- The Amended Rule also includes a series of requirements intended to ensure that the dealer has the appropriate personnel to adequately protect and secure data and that those personnel are able and qualified to enact the dealership's security program. These include:
  - **General employee training**
    The Amended Rule requires dealers to "provide their personnel with "security awareness training that is updated to reflect risks identified by the risk assessment."
  - **The use of qualified information security personnel**
    The Amended Rule requires dealers to "utilize qualified information security personnel," employed either by them or by affiliates or service providers, "sufficient to manage [their] information security risks and to perform or oversee the information security program."
  - **Specific training for information security personnel**
    The Amended Rule requires dealers to "provide information security personnel with security updates and training sufficient to address relevant security risks." This requirement is separate and in addition to the "general training" requirement above.
  - **Verification that security personnel are taking steps to maintain current knowledge on security issues**
    Finally, under this section, the Amended Rule requires dealers to "verify that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures." The FTC states that "this requirement was intended to complement the proposed requirement regarding ongoing training of data security personnel, by requiring verification that such training has taken place.

Appendix Cont.

Overseeing and Monitoring Service Providers

- The Amended Rule also requires dealers to "Oversee service providers, by:
  - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue.
  - Requiring service providers by contract to implement and maintain such safeguards; and
  - Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards."
- This requirement is like existing requirements regarding service providers, except that it also expressly contains a requirement to monitor and assess service providers after the onboarding stage. This will likely include audits and other formal and documentable assessment steps.

Required Written Incident Response Plan

- The Amended Rule requires dealers to adopt a written incident response plan that specifically addresses:
  - The goals of the plan
  - The internal processes for responding to a security event
  - The definition of clear roles, responsibilities and levels of decision-making authority
  - External and internal communications and information sharing
  - Identification of requirements for the remediation and associated control of any identified weakness in information systems
  - Documentation and reporting regarding security events and related incident response activities
  - The evaluation and revision as necessary of the incident response plan following a security event

Required Annual Written Report to the Board

- Amended Rule requires dealers to "Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body." This report must cover specific delineated areas, including:
  - The overall status of the information security program and the dealer's compliance with the Safeguards Rule, and
  - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

About Nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @Nuspire

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks