Amended Final Safeguards Rule
Preliminary FAQs

On October 27, 2021, the FTC **issued** its long-awaited, final amendments to the FTC Safeguards Rule ("Rule"). The **Rule** contains a significant number of new and expanded procedural, technical, and personnel requirements that financial institutions, including dealers, must satisfy to meet their information security obligations.[1]

Regulatory Affairs will develop comprehensive compliance guidance for NADA members.

In the meantime, dealers are encouraged to reach out to their technology vendors as soon as feasible to ensure they are taking the necessary steps to comply with the new requirements.

Attached are answers to several preliminary dealer questions, some details about what the Amended Rule requires (Exhibit A), and a copy of a third-party cost study commissioned by NADA that outlines the estimated costs for compliance with many of the new requirements (Exhibit B).

Q What is the Safeguards Rule?

A The Safeguards Rule ("Rule") is a federal data security rule that requires financial institutions (including dealers) to have measures in place to keep customer information secure. In addition to developing their own safeguards, dealers are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

Q What does it require?

A The specific requirements of the current Rule are outlined in several NADA guides, but, in brief, the Rule requires financial institutions to "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."

In other words, you should today have a written document that you have developed for your store, after reviewing your systems and the information you maintain, that contains a series of steps you are taking to protect that data.

Notably, this current requirement allows dealers the flexibility they need to protect data in a manner that is appropriate to the size and scope of their operations.

Q Is the Safeguards Rule new?

A The Rule itself is not new; it has been in effect for nearly 20 years. What is new is that the FTC has amended the Rule. The FTC began its efforts to amend the Rule in 2019, and NADA submitted several sets of detailed comments, participated in a Public FTC workshop, and undertook extensive additional advocacy in response to the proposed amendments.

Q Why is the FTC changing the Rule?

A The FTC proposed amendments to the current Rule in response to pressure to address "recent high profile data breaches." While the FTC responded favorably to several concerns with the proposed Rule that NADA identified (including by eliminating the proposed requirement that financial institutions hire or retain a Chief Information Security officer (CISO)), it nonetheless included in the Amended Rule a series of new technical requirements.

1 The Amended Rule is final, but in connection with the proposed rule, the FTC is also considering a proposal that financial institutions notify the Commission of detected "security events." (Defined as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system.") The Commission is issuing a Notice of Supplemental Rulemaking that proposes adding such a requirement. NADA will be submitting comments to the FTC and will provide further guidance as it becomes available.

Q What has changed?

A Some of the specific changes are listed in Appendix A below but, broadly speaking, 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.

Q When is this effective?

A Dealers, and all of their service providers that access any customer data, will have one year from the Amended Rule's publication in the Federal Register (which is expected shortly) to comply with the majority of the new requirements.

Some of the changes in the Amended Rule take effect 30 days after publication. Although the Commission notes that "These remaining requirements largely mirror[] the requirements of the existing Rule." However, as dealer action may be necessary on several of these changes in the next 30 days, dealers should consult with their counsel to ensure compliance with the current rule and any such changes.

The sections that require compliance within 30 days are:

- 314.4(b)(2)—additional periodic risk assessments;[2]
- 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, and;
- 314.4(g)—Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d).

2 This is the only "new" requirement not expressly found in the current Rule.

Q Are there any exceptions?

A 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. We believe that 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.

Q What about my OEM?

A 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.

Q Will this be expensive for dealers?

A There is no clear answer to that question, but the new requirements are certainly extensive, complicated, and for many dealers will add significant costs. Note that during the time the FTC was considering the proposed rule, NADA submitted the results of an independent third-party cost study, conducted by an experiences IT services firm, that detailed the estimated costs to comply with many of the new requirements for the average sized dealership. A summary of that study is attached at Exhibit B. Importantly, several of the requirements outlined therein have been clarified or amended, or do not appear in the Amended Rule. We are hopeful that only a very few dealers will face all of these costs (as many dealers already meet some of the new requirements), and we certainly hope and expect that the market will provide efficiencies that do not exist today. However, that summary provides an estimate of what many dealers will be facing in terms of potential additional costs to comply with the Amended Rule.

Nothing in this FAQ document or the accompanying Exhibits is intended as legal advice. Dealers must consult with their attorney or other professional advisors regarding their own facts and circumstances, and application of the Amended Safeguards Rule to their operations. This document is only an overview of one federal regulatory requirement in this area and does not address state or local law in any way.

APPENDIX A

Overview of Changes in the Amended Rule

The following is a brief overview of the primary new requirements dealers[3] must undertake pursuant to the Amended Safeguards Rule. Each of these raise a number of complicated and multi-faceted implementation questions, answers to which will need to be developed in more comprehensive guidance. In addition, the Amended Rule makes a number of material changes to the definitions used in the Safeguards Rule, as well as the scope of the Rule itself that will also require further analysis and guidance. With those and other caveats in mind, below are several of the more material changes likely to require action by many dealers (and their vendors) pursuant to the Amended Rule.

1 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.

2 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.

3 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."

4 Undertake a required data and systems inventory

The Amended Rule requires dealers to "[i]dentify 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."

5 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.

6 Requirement to Adopt Secure Development Practices and Assess Externally Developed Applications

The Amended Rule requires dealers to "[a]dopt 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."

7 Multi-Factor Authentication

The Amended Rule requires dealers to "[i]mplement 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.

3 The term "dealers" is used for convenience rather than restating "all financial institutions, including dealers". Each of these duties applies to all "financial institutions," including dealers.

8 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."

9 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."

10 Required Change Management Procedures

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

11 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."

12 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."

13 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 "[u]tiliz[e] 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 "[p]rovid[e] 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 ""[v]erify[ ] that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures."

  The FTC states that "[t]his requirement was intended to complement the proposed requirement regarding ongoing training of data security personnel, by requiring verification that such training has taken place."

14 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 similar to 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.

15 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 of any identified weaknesses in information systems and associated controls;
- documentation and reporting regarding security events and related incident response activities; and
- the evaluation and revision as necessary of the incident response plan following a security event.

16 Required annual written report to the Board

The 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.

APPENDIX B

Overview of NADA Cost Study for Proposed Changes to the Safeguards Rule

** This cost study was based on the requirements in the proposed rule as issued by the Commission in 2019. It is included for general information only, and it is not intended to suggest any requirement or minimum. It is a third-party IT firm's estimate of the potential impact on the average dealer and is not from the FTC. In addition, it is important to note that many of the requirements have been clarified or limited, and that the first item, "Appointing a CISO," has been removed from the Amended Rule, and replaced with the "Qualified Individual" requirement.

NADA COST STUDY: AVERAGE COST PER U.S. FRANCHISED DEALERSHIP

Proposed Change[i]	One-Time Up-Front Cost	Annual Cost
Proposed Paragraph (a) – Appointing a CISO to increase program accountability.	$27,500	$51,000
Proposed Paragraph (b) – Requiring that the Information Security Program Be Based on a Written Risk Assessment.	$26,500	$26,500
Proposed Paragraph (c) (2) – Required Data and Systems Inventory	$16,750	$10,250
Proposed Paragraph (c) (4) – Requirement to Encrypt Data at Rest and in Transit.	$9,000	$8,500
Proposed Paragraph (c) (5) – Requirement to Adopt Secure Development Practices	$9,000	$37,500
Proposed Paragraph (c) (6) – Required Multi-Factor Authentication	$33,750	$18,500
Proposed Paragraph (c) (7) – Requirement to include Audit Trails.	$30,000	$18,000
Proposed Paragraph (c) (8) – Requirement to Develop Secure Disposal Procedures	$30,000	$10,800
Proposed Paragraph (c) (9) – Required Adoption of Procedures for Change Management	$30,000	$2,000
Proposed Paragraph (c) (10) – Required Unauthorized Activity Monitoring	$20,000	$29,000
Proposed Paragraph (d) – Required Penetration Testing and Vulnerability Assessments	$20,125	$23,125
Proposed Paragraph (e) – Required Employee Training and Security Updates	$2,100	$14,875
Proposed Paragraph (f) – Required Periodic Assessment of Service Providers	$14,250	$11,250
Proposed Paragraph (h) – Required Incident Response Plan	$16,000	$6,625
Proposed Paragraph (i) – Required Written CISO report	$9,000	$9,000
Total Cost Incurred/ Dealership[ii]	**$293,975**	**$276,925**
Total Cost Incurred Across All Dealerships[iii,iv,v]	**$2,236,267,825**	**$2,106,568,475**

Disclaimer: *Nothing in this FAQ document or the accompanying Exhibits is intended as legal advice. Dealers must consult with their attorney or other professional advisors regarding their own facts and circumstances, and application of the Amended Safeguards Rule to their operations. This document is only an overview of one federal regulatory requirement in this area and does not address state or local law in any way.*