

# An Auto Dealer's Guide to the FTC Safeguards Rule

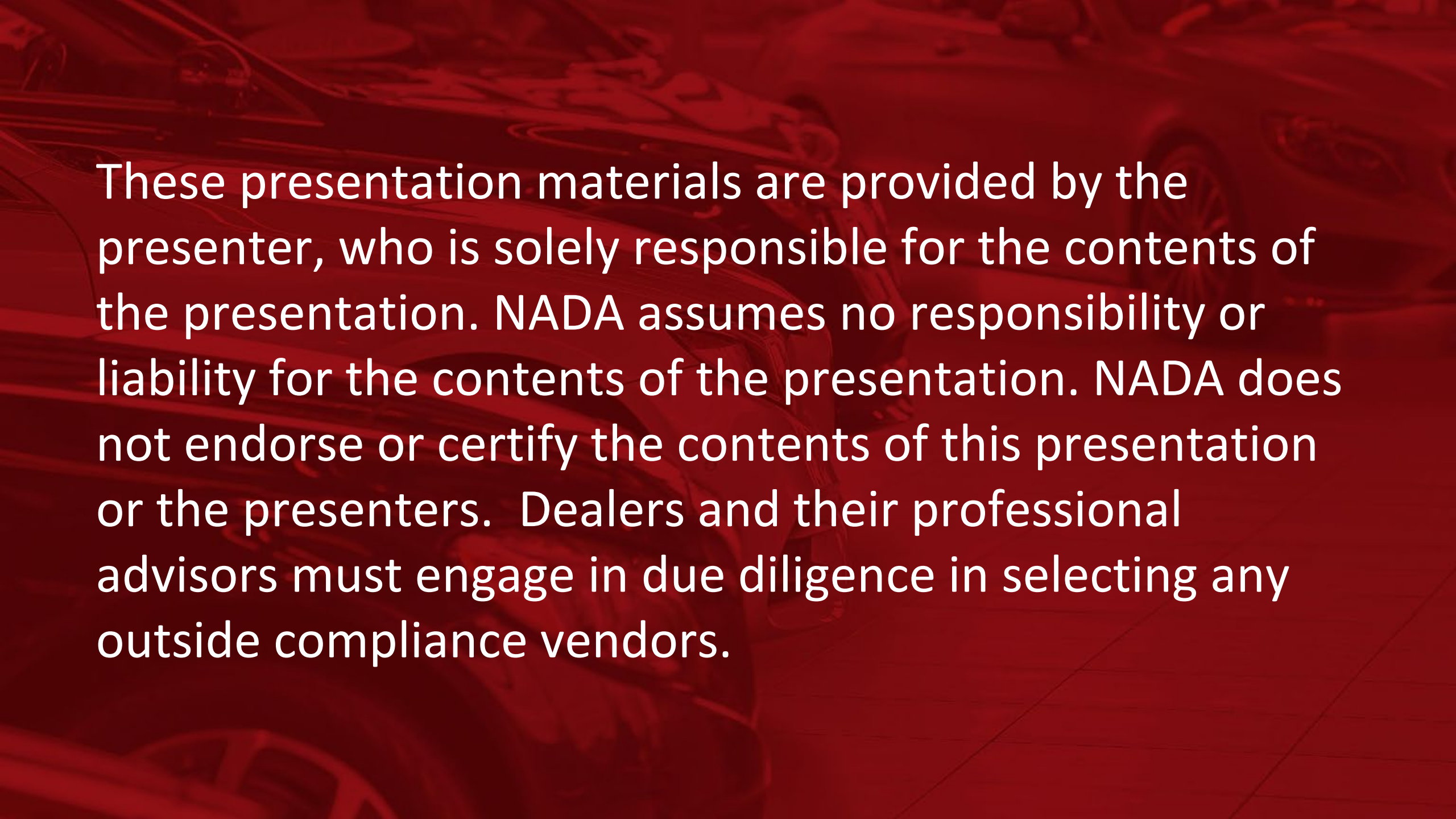


**Louis Evans**  
*Senior Product Marketing Manager*  
Arctic Wolf  
[Louis.evans@arcticwolf.com](mailto:Louis.evans@arcticwolf.com)



**Mike Bertolini**  
*IT Director*  
Bill Jacobs Motorsport  
[mike.bertolini@billjacobs.com](mailto:mike.bertolini@billjacobs.com)





These presentation materials are provided by the presenter, who is solely responsible for the contents of the presentation. NADA assumes no responsibility or liability for the contents of the presentation. NADA does not endorse or certify the contents of this presentation or the presenters. Dealers and their professional advisors must engage in due diligence in selecting any outside compliance vendors.

# Agenda

- 01 Overview of the FTC Safeguards Rule**
- 02 The Nine Security Requirements for Auto Dealers**
- 03 Cost of Implementing vs. Non-Compliance**
- 04 Solution: How Can an MDR Partner Help?**
- 05 Questions?**

# Overview of the FTC Safeguards Rule



- With roots in the Gramm-Leach-Bliley Act (GLBA), the Safeguards Rule expands the definition of financial institution to include a broader swath of industries that provide financial services to customers, which now includes auto dealers.



- Dealerships are required to achieve compliance with the new FTC Safeguards rule by December 9<sup>th</sup> or face fines up to \$50K.



- For auto dealerships, the rule requires detailed procedures and specific criteria that auto dealers must implement to provide better protection and to curb data breaches and cyberattacks that could jeopardize sensitive customer data.



- Dealerships not only must implement changes to protect their own consumer data, but also must have a formal employee training program and third-party audits in place to ensure their entire list of vendors also are following these guidelines.

# 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

1

**Designate a “qualified individual” to implement and supervise your dealership’s information security program.**

**What this means:**

- Requires a single employee or outside contractor fulfill the role of “qualified individual,” vs multiple employees as was previously permitted.
- This person does not have to implement the program, but should be responsible for ensuring that the IT department or outside vendor follows protocol.

**Recommendation:**

*Whether you use an employee or an external partner to implement this element, ensure that at least one additional employee – beyond your qualified individual – is informed and regularly updated on the status of your program to ensure continuity and eliminate the risk of critical knowledge loss caused by leave or discontinued service.*



# 2

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

**Conduct periodic risk assessments to inform and guide the continued updating and enforcement of your information security program.**

**What this means:**

The updated Safeguards Rule broadens the criteria for what risk assessments must include and requires written record of the risk assessment is maintained:

- Evaluation of identified security risks or threats
- Assessment of the quality of your existing security controls in context of security risks
- Explanation of how the identified risks will be mitigated

**Recommendation:**

*A helpful way to organize a risk assessment is to trace customer information throughout its life cycle at your dealership. Begin where the information is gathered and consider every point where it is processed, recorded, transmitted, and stored.*

# 3

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

**Implement customer information safeguards to control the risks identified in the risk assessments.**

**What this means:**

Dealerships are required to implement the following safeguards, among other activities, to address identified risks from their risk assessments:

- Access controls
- Systems inventory
- Encryption
- Secure development practices
- Multifactor authentication
- Disposal procedures
- Change management procedures
- Monitoring

**Recommendation:**

*Customer information is defined very broadly under the Safeguards Rule, so the safest practice is to consider any information a customer provides (even simply their name) as covered customer information. Many of these controls may be easier to implement, maintain, and oversee with the support of security partners.*

# 4

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

### **Regularly monitor and test your safeguards.**

**What this means:**

This element of the Rule requires regular testing or continuous monitoring of the effectiveness of the safeguards in place, including detecting actual and attempted attacks and intrusions on your dealership's information systems.

Dealers have the choice to select either continuous network monitoring or annual penetration testing along with twice-annual vulnerability assessments to meet the requirements of this element.

**Recommendation:**

*As you evaluate your options for meeting the requirements of this element, it is worthwhile to assess continuous monitoring solutions as an effective way to meet requirements and achieve security and vulnerability visibility.*



# 5

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

### **Train your staff.**

#### **What this means:**

Relatively self explanatory, the new Rule requires that employee security awareness training be updated over time based on evolving risk assessments or changes in a dealership's practices. It also requires that security personnel receive "security updates and training sufficient to address relevant security risks," and dealerships keep verification that training requirements have been met.

#### **Recommendation:**

*Security awareness training is a relatively established segment of the cybersecurity solution space. But established vendors may simply offer training and testing materials, leaving IT staff at organizations the heavy workload of managing and updating a security awareness program. Make sure you understand the implementation activities required before selecting a security awareness solution to meet this requirement.*

# 6

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

### **Monitor your service providers.**

#### **What this means:**

This element requires that dealers conduct due diligence on the security measures of all vendors that process, collect, store, or access any customer data on its behalf.

- Proactively reviewing and evaluating vendors' security measures before vendors are engaged, and then conducting an annual security audit or assessment of their measures.
- Updating all contracts with vendors that process, collect, store, or access your customer data to include terms that require information security practices commiserate with information security standards used within your dealership

#### **Recommendation:**

*Consider adding the following requirements to your contracts with external service providers to help meet the requirements of this element:*

- *The information security standards of your dealership and your expectations for service providers to meet your standards*
- *The vendor's security measures for protecting customer data and an ongoing obligation to maintain those security measures.*
- *How the service provider will be monitored to ensure compliance with security obligations*
- *When scheduled, periodic security reassessments will take place*

# 7

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

**Keep your information security program current.**

**What this means:**

Changes in your business operations, IT environment, risk assessment, personnel, and the evolving threat landscape will all have a material impact on your security operations program and necessitate updates.

**Recommendation:**

*Your qualified individual (either employee or external vendor) will need to synthesize the outputs from your information security program's safeguards required by the Rule, including risk assessment, controls monitoring, and vulnerability visibility to understand if your safeguards currently in place effectively address current risks and threats to your environment.*

# 8

## 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

### **Develop and implement a written incident response plan.**

#### **What this means:**

The amended Rule requires a written incident response plan designed to address how a dealership will respond to and recover from any security event that would impact the confidentiality, integrity, or availability of customer information.

#### **Recommendation:**

*Ensure that physical copies of your incident response plan are kept in secure yet accessible locations, as they are of no use if they are kept only in digital format on devices or a network you are unable to access in the event of a breach of your IT systems.*

# 9 Security Requirements of the FTC Safeguards Rule

*Requirements are based off Section 314.4 Elements*

# 9

**Require your qualified individual to report to your board of directors.**

**What this means:**

the qualified individual at your dealership must provide a written report to your board of directors at least once a year. In the event your dealership does not have a board of directors, this report must be submitted to your dealership's senior officer, who is responsible for your security program.

**Recommendation:**

*Make sure the security solutions you invest in aren't just able to fulfill a particular requirement, but that the solution is also capable of providing the corresponding documentation required to support this board-facing report.*



# The cost of non-compliance

*Not ensuring compliance can ultimately prove more costly than compliance.*

- FTC has established penalties for non-compliance that can go up to \$46,000 per violation per day.
- Ransomware is a common and costly type of attack hitting auto dealerships. The average ransomware payment was up 8% in the first quarter of 2022 to \$228,125 with downtime of 24 days. That's an average, though, and the individual demand could range into the millions.
- The costs of an attack go beyond just monetary damages and ransomware payments: dealerships reputations are at stake. With dealerships often relying on online reviews and social media ratings, a breach of customer data can be significantly damaging to the reputation and long-term business of a dealership.



# **Solution: How Can an MDR Partner Help?**

- Dedicated team members who set up regular meetings to review your overall security posture and find areas of improvement that are optimized for your environment.
- Monitor environments 24x7 to detect, review and respond to cybersecurity threats.
- Provide continual vulnerability assessments.
- Identify threats targeting network or cloud applications.
- Conduct cybersecurity awareness training for security teams and employees.



# Questions?

# An Auto Dealer's Guide to the FTC Safeguards Rule



**Louis Evans**  
*Senior Product Marketing Manager*  
Arctic Wolf  
[Louis.evans@arcticwolf.com](mailto:Louis.evans@arcticwolf.com)



**Mike Bertolini**  
*IT Director*  
Bill Jacobs Motorsport  
[mike.bertolini@billjacobs.com](mailto:mike.bertolini@billjacobs.com)







**NADA**

The logo features the word "NADA" in a bold, white, sans-serif typeface. Below the text is a graphic element consisting of two parallel white wavy lines that follow the contour of the letters. The entire logo is centered on a dark red background that has a semi-transparent overlay of a car dealership lot with several vehicles parked.