WHITEPAPER

A Starting Point for Safeguards Compliance

Is Your Safeguards Program Bulletproof?

MOSAIC
CYBER SECURITY

1.

What must a dealership do to come into compliance?

The list of requirements under the Rule is extensive, and is well-described in NADA's Amended Safeguards Rule Preliminary FAQs

The requirements include, but are not limited to:

- Qualified Individual
- Training and Testing Employees
- Overseeing Service Providers
- Written Risk Assessment
- Written Information Security Program ("WISP")
- Access Controls
- Secure Development Practices
- Secure Disposal Practices
- Change Management Procedures
- Written Incident Response Plan
- Annual Report
- Data Encryption
- Multifactor Authentication ("MFA")
- EDR or Pen Test + VA
- Systems Monitoring and Logging
- Vulnerability Assessments ("VAs")
- Data and Systems Inventory
- Unauthorized Activity Monitoring

2.

What qualifications must a Qualified Individual have?

The dealership must designate a single individual to fill this role and bear responsibility for the program.

That person doesn't need to be qualified to perform the necessary duties, just qualified to competently oversee that the necessary duties are performed and documented. The actual duties may be performed by a third-party, such as a Managed Service Provider ("MSP"), but responsibility will remain with the designated dealership representative.

3.

Must I draft a WISP from scratch?

No – NADA has an excellent template in their *Dealer Guide to the FTC Safeguards Rule*. It's free for NADA members, or may be purchased by non-members for $89. You can download it at https://www.nada.org/safeguardsrule/

4.

What's a Service Provider?

A Service Provider is any person or entity that receives, uses, processes, stores, or has access to your customers' information through their providing services to your dealership.

Service Providers include banks, credit unions, F&I providers and administrators and their agents, and outside IT support. Even your janitorial service could be considered a Service Provider.

5.

Continuous network monitoring, or annual penetration testing and twice-annual vulnerability assessments?

Dealers may include in their WISP either continuous network monitoring, or annual penetration testing and twice-annual vulnerability assessments. What's the difference?

Continuous monitoring does just that - it monitors a computer network 24/7 and immediately detects breach attempts, allowing rapid response. Vulnerability assessments ("VAs") just take a picture of network risks at a specific moment in time. Put another way, continuous monitoring actually protects a network, while VAs periodically identify risks to the network. In fact, continuous monitoring functions as a continuous VA.

VAs may seem an attractive option because that approach is cheaper than continuous monitoring. But penetration testing, which are required if VAs are used, is quite expensive if done right. A meaningful external penetration test requires both a VA and at least 40 man-hours of human attention at $150 - $300 per hour, so going that route may be a false economy.

6.

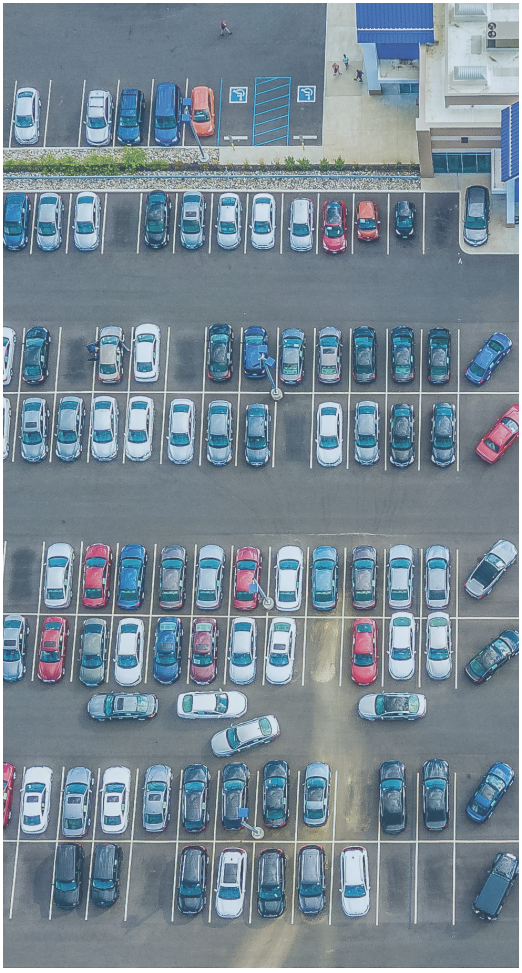
How much does all this cost?

That's a little like asking "How much does a car cost?" It depends on many factors, including size of a dealership's computer network, the dealership's IT resources (internal and external), and the specific approach a dealer wants to take.

Expect to pay between $1,500 and $6,000 per rooftop per month, all in, depending on the size of your dealership and its sales volume (the higher the sales volume, the bigger the network to be protected).

Beware of "cheap" solutions! It is unlikely any one vendor will have a complete turnkey solution, and a false sense of security can be very expensive in the long run.

Before engaging any vendor's solution, check with a cybersecurity insurance provider to see if the proposed solution is defensible and insurable. If it isn't, keep shopping.



7.

What happens if I don't come into compliance?

While FTC enforcement actions, consent orders and fines ($46,517 per violation) are possible, they are unlikely. Far more likely are consumer class action lawsuits, because the FTC considers a violation of the Safeguards Rule to constitute a deceptive trade practice. The first federal class action on this basis against a dealership group was filed in February of 2022 – less than a month after the revised Safeguards Rule went into effect! And the possibility remains that banks won't buy the paper of dealerships that can't demonstrate compliance with the Rule - the Safeguards Rule applies to banks, too.

8.

Does the Safeguards Rule apply to my vendors?

If a vendor has access to your customers' information, then they are considered Service Providers and the Rule applies to them.

9.

Does the Safeguards Rule apply to the banks that buy my paper?

Yes.

10.

How do I confirm my Service Providers comply with the Safeguards Rule?

At a minimum, request a copy of each Service Provider's WISP. Using a Service Provider questionnaire is a reasonable additional step you should take; these are included in many software programs that perform and track this function.

11.

What must I do with Service Providers that can't demonstrate they comply with the Safeguards Rule?

Fire them and replace them with Service Providers that can demonstrate their compliance with the Rule. A Service Provider's violation is the dealer's violation.

12.

How do I get started?

Go to Mosaic's website (https://www.MosaicCS.com) and complete the Safeguards Status Questionnaire online, or download it and return it to responses@MosaicCS.com. Either way, Mosaic will take it from there. The most important thing is to decide to do something about Safeguards compliance and take the first concrete step. This is it.

Mosaic's Solution covers all the requirements of the revised FTC Safeguards Rule and offers a-la-carte options so you can build a program that fits your needs.

STEP 1

Fill out a Safeguards Status Questionnaire.

Fill Out Online

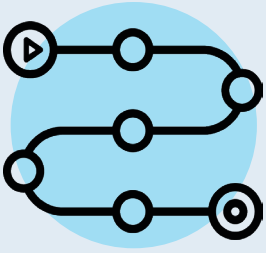
Download

STEP 2

We'll contact you to provide a complimentary consultation based on your responses.

STEP 3

Build your custom roadmap for complete compliance.



LEARN MORE

MAKING VIRTUE PROFITABLE

Learn more about our Safeguards Solution at ***mosaiccs.com****.*

POWERED BY MOSAIC CYBER SECURITY