WHITEPAPER

A Starting Point for Safeguards Compliance for Agents

Is Your Safeguards Program Bulletproof?

MOSAIC
CYBER SECURITY

1.

What must a dealership do to come into compliance?

The requirements include:

- 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.

To adequately protect dealership data, what Safeguards should an agency have in place?

While not defined by the rule, best practices indicate that the following Safeguards are the best place to start:

- Training and Testing Employees
- Security Awareness Training
- Written Information Security Program (“WISP”)
- Access Controls/Physical Safeguards
- Secure Disposal Practices
- Data Encryption
- Multifactor Authentication (“MFA”)
- Continuous Monitoring
- Firewall
- Robust Anti-virus and Anti-malware

3.

Who should be a dealership's Qualified Individual?

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.

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.

5.

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

Dealers must implement either continuous 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.

6.

How much does all this cost?

There is always concern about the cost of compliance. For example, not all pen tests nor EDR services are equal. A good pen test typically takes place over several days and can cost between $10,000 - $30,000 per test. Beware of “free” or “fully automated” pen tests. While tempting, they lack the expert insight and recommendations that only a live pen test professional can provide to ensure your vulnerabilities are truly addressed.

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.

7.

What happens if a dealership doesn'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!

8.

How will dealers confirm their Service Providers are complying with the Safeguards Rule?

At a minimum, dealers will request either a copy of their service providers' WISPs or a Safeguards Agreement detailing how the service provider protects the dealer's customer information. The dealer with then review the documents to ensure the service provider is adequately protecting the dealership.

9.

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

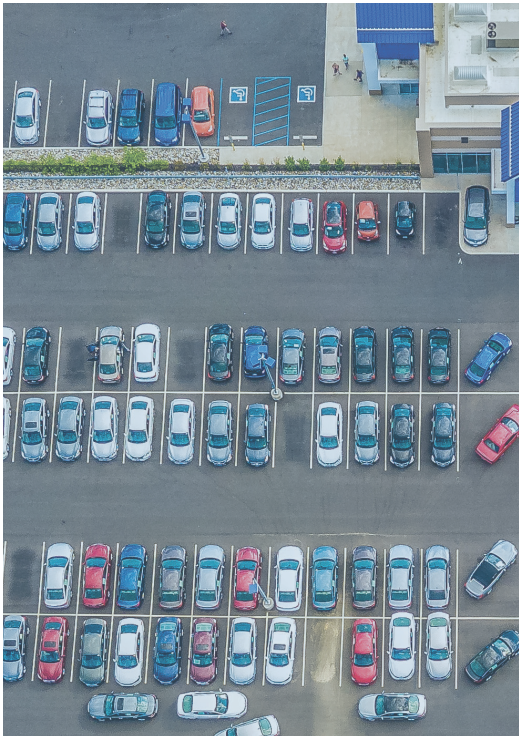
Fire them and replace them with Service Providers that can demonstrate their compliance with the Rule. A Service Provider's violation is the dealer's violation.

10.

How do I get started?

Go to Mosaic's website (https://www.MosaicCS.com/quote) and complete the Safeguards Status Questionnaire. Mosaic is able to help both agents and dealers effectively comply with the Safeguards Rule. The most important thing to do is get started now.

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

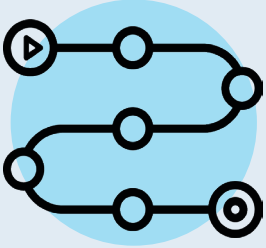
Download

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

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.

MAKING VIRTUE PROFITABLE

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

POWERED BY MOSAIC CYBER SECURITY