

A man with short, wavy blonde hair and a light beard, wearing a grey suit jacket over a white shirt, is looking down at his wrist with a slight smile. The background is a blurred office setting. The entire image has a semi-transparent blue overlay.

How Much Time Does Safeguards Compliance Take?

Don't let hours become months

The truth about the time you will need to set up your Safeguards and when to get started.

Enforcement for the FTC Safeguards Rule begins June 9th. Compliance is mandatory and failure to do so is viewed by the FTC as a deceptive trade practice. The question is how long can your dealership afford to wait before implementing its Safeguards? This whitepaper will reveal when to consider getting started and how long it takes to set up each Safeguards requirement.

When to set up your Safeguards:

When the FTC extended the Safeguards deadline for some items back in November '22, they did so "in response to reports of personnel shortages and supply chain issues." This suggests that even the most competent dealerships were struggling to get everything in place, despite knowing about it since January 10, 2022. That is 11 months of lead time! Let us look at why that is.

How long does each requirement take:

While every dealership has been given the same set of requirements, there are a number of ways to address them. As a result, how a dealer satisfies them ultimately determines both the effort and effectiveness of a dealership's Safeguards. To best answer the question "how long does it take to comply with Safeguards", let's take a closer look at some of the requirements. Here are three examples illustrating the efforts involved:

Service Provider Oversight

First, there is the most time-consuming process of all – overseeing your service providers. Dealers must review their vendors, confirm if they have access to dealership customer information, and ensure they are adequately protecting it.

Most dealerships have 16 or more service providers that qualify. Someone at your store, likely the QI, would reach out to each service provider, collect the necessary documentation, read through it and approve that provider based on their security measures. This can be very time consuming, and responses limited - adding even more follow up to your QI's workload. Completing this task could easily take eight hours or more. Finally, if a service provider is unable or unwilling to protect your dealership's data to your standards, you will then need to find and implement a new provider for that function.

Continuous Monitoring

Continuous monitoring is perhaps the most impactful security requirement. Dealers may satisfy this in one of in two ways: Endpoint Detection and Response (EDR) or A Penetration test paired with vulnerability scanning at least every six months. We recommend EDR because it protects your dealership, while the latter option does not and may cost more. [Learn More](#) EDR is commonly set up by installing a software "agent" on all your computers. Once installed, the technology will monitor your devices 24/7 to detect and alert you of cyber threats. Hint: A good EDR will come with a team of cyber security humans (SOC) that will also remediate the threats for you. Installing an agent typically takes 2-3 minutes per computer. Keep in mind mass deployment or RMM tools can significantly reduce the installation burden but will require initial setup. It may take a single point, with 70 computers, 3-4 hours to set up EDR completely. The AI will also need a few eeks of calibration to ensure optimal protection post-installation.

Multifactor Authentication & Encryption

The Rule requires dealers to implement multifactor authentication (MFA) for any individual accessing any information system and encrypt customer information both in transit and at rest. Solving for these often necessitates dealer-specific solutions resulting in the greatest variety of outcomes and cost. For example, a dealer's DMS and CRM may already have MFA and encryption, but the salespeople still use their personal email. This may require the dealer to implement Microsoft Office 365 or Google Workspace which natively includes MFA and encrypted emails. When transitioning email platforms, give yourself at least two full months



and the cost for MSP support is unique to the dealer's size and license selection. Bottom line? This may be the most involved and expensive requirement, or... it may be the least. It all depends on what tools you currently have in place.

Seek Expert Help to Streamline the Process

It's easy to quickly become frozen by the size and scope of requirements. Take courage, there is help! You can save significant time and money by partnering with a company that specializes in dealership Safeguards compliance. In addition, you may receive peace of mind knowing it's done right. Keep in mind that your dealership will still need a designated qualified individual to oversee and implement the security program, and ultimately, it's still the dealership that's responsible in the eyes of the FTC.

A Comparative Time Estimate for Safeguards Requirements

To help illustrate the time necessary for each Safeguard, we've created a comparison chart. It highlights the time you can expect to take for a single-point dealership to set up everything on their own, or with a partner. In this example, we've used Mosaic Compliance Services as the partner.

Don't Wait, Start Now

Your worst enemy is doing nothing. Whether you need to implement one requirement, or all of them, don't wait to get started. The Safeguards Rule is quickly becoming the most expensive liability risk a dealership can face. Procrastination can lead to costly data breaches and legal battles. Start addressing the Safeguards requirements today and consider partnering with an expert to ensure a smooth and efficient compliance journey.

Streamline Your Safeguards Compliance with Mosaic

Discover the Benefits and Take Our Questionnaire

[Click Here](#)

Service	Dealer Setup Alone	Dealer Setup with Mosaic
Risk Assessment	240 Minutes	60 Minutes
Service Provider Oversight	300 Minutes	60 Minutes
Vulnerability Assessments	130 Minutes	60 Minutes
Endpoint Detection and Response	240 Minutes	180 Minutes
MFA & Encryption	TBD	TBD
Security Awareness Training	120 Minutes	15 Minutes
QI Training	180 Minutes	5 Minutes
Information Security Program	240 Minutes	30 Minutes
Annual Report	120 Minutes	0 Minutes
Total Hours	26.2 Hours	6.8 Hours

19+
Hours of work potentially saved when setting up Safeguards with Mosaic.