Myths & Misconceptions About the Revised FTC Safeguards Rule

By Chris Cleveland, CFO and
Hao Nguyen, Esq., General Counsel
ComplyAuto

By now, almost all dealerships are aware that the Federal Trade Commission (FTC) revised the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule for the first time in 20 years, with the new regulations going into effect on December 9, 2022. In conjunction with these new regulations, the FTC released a 145-page publication of comments and clarifications to certain aspects of the new Rule and dealers have been bombarded with seminars, webinars, articles, and sales pitches from various sources about its interpretation. Unfortunately, with all that information has come some misinformation as well. So, let's bust the most common myths and misconceptions about the revised Safeguards Rule.

1. **MYTH # 1**: Dealers don't need to perform penetration testing or vulnerability scanning if they're doing 24/7 threat detection monitoring through an EDR, MDR, or SIEM tool.

The regulations create an exception to annual penetration testing and biannual vulnerability scans if the dealer is performing "continuous monitoring." However, many IT companies and Managed Service Providers (MSPs) have gotten into the habit of liberally throwing around the term "continuous monitoring" to describe their EDR, MDR, and SIEM tools. We believe that many of those tools may not satisfy true "continuous monitoring" requirement in the way that it is defined by the FTC's regulations. Not that those tools aren't valuable -- they are in fact very valuable and we highly recommend them -- it is just unlikely that it exempts you from completing the required penetration tests and vulnerability assessments. The regulations define "continuous monitoring" as a system that performs the following items in a real-time, ongoing manner:

1. Monitoring for security threats;
2. Detection of misconfigured systems; and
3. Vulnerability assessments.

While most tools do the first item (monitoring for security threats), the vast majority are not performing items two and three (realtime, ongoing configuration scanning and vulnerability assessments). There are tools out there that offer various packages that can do true continuous monitoring (e.g., Splunk, DataDog, Qualys, to name a few), but they're going to be very expensive. It was noted in an FTC Workshop that the type of continuous monitoring referenced in the Safeguards Rule could cost a small to midsized company around $600,000 *per year*. The FTC even implies that you'd need dedicated and experienced staff to monitor the logs and activity by a system around-the-clock, 24/7/365. In fact, the prohibitively high cost is *precisely* why the FTC allows businesses to complete an annual penetration test and biannual vulnerability assessment as an alternative to continuous monitoring.

In short, most dealers will not be performing "continuous monitoring" as contemplated by the

new regulations and will therefore still need to perform an annual penetration test and biannual vulnerability assessment.

2. **MYTH # 2**: Dealers need to hire a full-time Chief Information Security Officer (CISO) or other security professional under the law.

While the originally proposed rules were contemplating requiring a CISO be appointed to oversee your information security program, this was ultimately replaced by a requirement that you simply appoint a single "qualified individual" at the dealership. No particular level of education, experience, or certification is defined by the Safeguards Rule. According to the FTC, dealers may designate any qualified individual who is appropriate for their business as based on their size and complexity. The purpose behind requiring designation of a single coordinator is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication.

Note that while the "qualified individual" must have ultimate responsibility for overseeing and managing the information security program, dealers may still delegate particular duties, decision making, and responsibilities to other staff members. Moreover, the Safeguard Rule does not require that this be the person's sole job – he or she may have other duties.

3. **MYTH # 3**: Dealers who host all their customer information in the cloud (e.g., in their DMS and CRM) don't need to worry about the new requirements because information security is the vendor's responsibility.

Actually, this is quite the opposite. Not only is it naive to think that all your customer non-public personal information (NPI) is in the cloud (think every time a sales or finance person downloads a bank "stip" from their email onto their PC), but the regulations specifically make verifying service providers' security the dealer's responsibility. For example, dealers are required to both (1) require their service providers by contract to implement and maintain reasonable safeguards and (2) periodically assess their service providers based on the risk they present and the continued adequacy of their safeguards. In any event, dealers are responsible for their own network security and implementation of the new Rule (e.g., encryption, multi-factor authentication, penetration testing, etc.), regardless of their service providers' level of involvement.

These are just a few examples of how a complex set of regulations with technical jargon can give rise to an abundance of inaccurate information. As a partner of the association, we here at ComplyAuto exist to help dealers navigate these complicated requirements and free up their limited resources (i.e. their time and their staff) so that they all can go back to doing what they do best – selling and servicing cars.

About ComplyAuto:

ComplyAuto is a Software-as-a-Service RegTech company that currently serves over 2,000 dealerships across the country. Built on over a collective 60 years of automotive compliance experience and led by a team of dealer owners themselves, ComplyAuto understands that unique dealer problems require unique dealer solutions rather than a “one-size-fits-all” product.

ComplyAuto’s suite of tools to help dealerships comply with state consumer privacy laws and all aspects of the federal Gramm-Leach-Bliley Act revised Safeguards Rule by reinforcing the dealership’s existing data protection and cybersecurity protocols through advanced tools such as penetration testing, vulnerability scanning, and dealer-specific phishing simulation software.

To schedule a product walkthrough, please go here: https://complyauto.com/schedule-demo