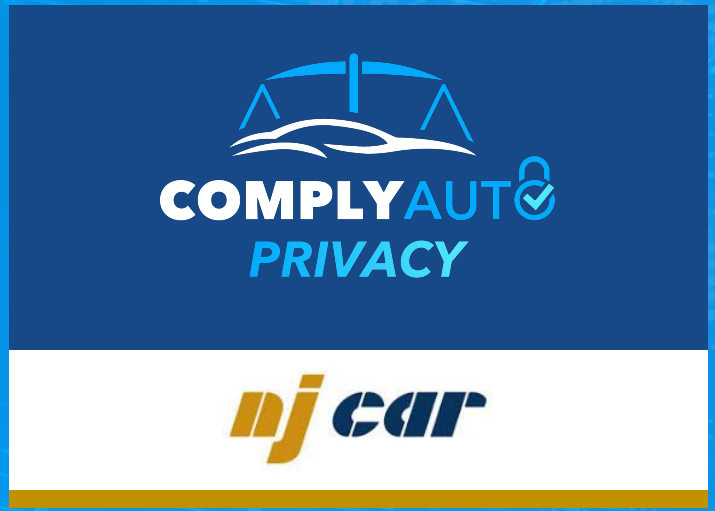
Complying with the Revised FTC Safeguards Rule

Practical Tips for Dealers



Presented on January 4, 2022

by Chris Cleveland

Compliance Director, Galpin Motors

CEO & Co-Founder, ComplyAuto

Chris Cleveland
Compliance Director, Galpin Motors
CEO & Co-Founder, ComplyAuto Privacy

John McCallan
Owner, Operator & Attorney, Raceway Ford
Partner, Kearny Mesa Ford & Kia of Sunroad Auto

Shane McCallan
Co-Founder, ComplyAuto Privacy
General Counsel, Raceway Ford *(former)*
Vice President, Auto Advisory Services *(former)*

Hao Nguyen
General Counsel, ComplyAuto Privacy
Staff Counsel, CNCDA *(former)*
Sr. Manager of Legal Affairs, KPA *(former)*

COMPLYAUTO PRIVACY

About Us

"By Dealers. For Dealers."

- 60+ years of combined dealership compliance experience
- We are responsible for privacy and information security at our dealership groups and have implemented compliance with the Revised Rules.
- ComplyAuto Privacy was created organically to solve problems faced by the owners at their own dealerships. Over **750** dealers currently using the ComplyAuto software.

Legal Disclaimer

This presentation is intended to be used as a compliance aid for motor vehicle dealers. Reasonable efforts have been made to ensure the accuracy of the following subject matter. No express or implied warranty is provided respecting the information contained in this presentation. The following material should not be used as a substitute for legal advice. If legal advice is required, the services of a competent professional should be sought. Each dealer must rely on its own expertise and knowledge of law when using the material provided.

BACKGROUND

- On October 27, 2021, the Federal Trade Commission (FTC) finalized revisions to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (“Revised Rule”) for the first time since the rule was issued in 2002.
- The Revised Rule if effective **January 10, 2022**
- The Revised Rules are detailed in a 145-page publication
- In its announcement, the FTC specifically names “automobile dealerships” as non-banking financial institutions that fall under the purview of these new revisions.
- The Revised Rule is extensive and imposes a series of new technical and administrative requirements on dealers. This includes, but is not limited to:
    i. internal penetration testing, vulnerability assessments, use of multi-factor authentication, data encryption, security awareness training, and the performance of written risk assessments.
- Dealers must act immediately to meet compliance with the new rules or otherwise risk penalties of up to $43,792 per violation.

APPLICABLE LAW OR REGULATION

16 CFR §314.4(c)(6)-(7), §314.4(c)(6)(h)(1)

Dealers must have a written Information Security Program and Incident Response Plan that is made available to employees.

FOUR WRITTEN POLICY REQUIREMENTS

The revised rule requires the following written policies:

1. Information Security Program
   - Existing programs must be updated in accordance with the new regulations.
2. Incident Response Plan
   - The regulations specify exactly what must be included in this plan.
3. Data Retention Plan
   - Must dispose of NPI after there's no longer a legal/business need
4. IT Change Management Procedures
   - Process to follow when major changes are made to IT infrastructure to ensure no security gaps

NJ CAR will be providing all attendees with a sample of the policies outlined above.

DESIGNATE A SINGLE PERSON TO OVERSEE YOUR ISP

Under the Revised Rule, you must appoint a single "Qualified Individual" to oversee your Information Security Program (“ISP”).

- It is generally recommended that this be a Chief Information Security Officer (CISO), IT Director, or person in a similar role. However, no prerequisite level of education, experience, or certification is defined by the Revised Rule.
- The purpose behind requiring designation of a single coordinator is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication. According to the FTC, splitting authority over an information security program between two or more people leads to failures of communications and oversight.
- Note that while this person must have ultimate responsibility for overseeing and managing the ISP, dealers may still assign particular duties, decisions, and responsibilities to other staff members.

APPLICABLE LAW OR REGULATION

16 CFR § 314.4(a)

Under the Revised Rule, dealers must appoint a single "Qualified Individual" to oversee their Information Security Program (“ISP”)

✖ Old Rule	✔ New Rule
Could be anyone at the dealership	Must be “qualified” in area of information security
Could be multiple individuals	Must be a single person
Known as the “Program Coordinator”	Referred to as the “Single Qualified Individual”

IMPLEMENT MFA FOR SYSTEMS WITH NPI

APPLICABLE LAW OR REGULATION

16 CFR § 314.4(c)(5)

Under the Revised Rule, dealers must require MFA for any system containing NPI.

Multi-factor authentication ("MFA") is an authentication system that requires at least two distinct authentication factors for successfully logging into a system. For example, **Password + Text Code**

MFA isn't just the law -- it can significantly help reduce your dealership's chances of a cybersecurity incident. According to a study by Microsoft, MFA blocks over 99.9 percent of account compromise attacks. There are three primary scenarios under which dealers will need to consider enabling MFA:

- **Third-party Applications**. Start by enabling MFA for all of your online or cloud-based applications and software that store or access customer NPI (e.g., your CRM, DMS, and credit-related systems).Popular dealer systems like DealerTrack and RouteOne already have a way to enable MFA for all users.
- **On-premises MFA**. If dealers are storing NPI on their own internal devices, networks, or servers (including an on-premises DMS), they should strongly consider enabling MFA on logins to the employees' workstations/operating systems.
- **Cloud Computing and Email Clients**. Most major email clients, like Microsoft 365 and Google (Gmail) natively support MFA. Make sure you enable MFA for all users accessing email, as NPI is commonly transmitted and stored via email. If your dealership is using Google Workspace or Microsoft Azure Active Directory, you should also enable MFA.

ENCRYPTING DATA AT REST & IN TRANSIT

APPLICABLE LAW OR REGULATION

16 CFR § 314.4(c)(3)

The Revised Rule requires that customer information be encrypted while in transit and at rest.

Put simply, encryption is the process of transforming usable data into an unreadable form. The Revised Rule requires that customer information be encrypted while in transit (e.g., while being sent over email or uploaded to a DMS) and at rest (e.g., while being stored on a computer's hard drive).

- **Dealer-owned Systems and Devices**. If any of the dealership's devices, such as desktops, laptops, tablets, or mobile devices store customer information, consider enabling the encryption of the hard drives on those devices.
- **Email Clients**. At a minimum, dealers should ensure the email client (e.g. Office 365, Google) is configured to send emails using TLS. Never allow employees to use their own personal email account for work, as it is difficult to control the security and encryption settings of those accounts.
- **Dealer-maintained Websites**. Most major website providers (e.g., Dealer.com, DealerInspire, Jazel, Sincro, etc.) have SSL certificates by default. However, if a dealership maintains any of its own websites, such as a group site landing page, ensure it has an SSL certificate (i.e., using an https:// instead of an http:// url). Not only is this a good security practice, but it also helps the site rank higher on search engines!

⌘ TECHNOLOGY TIP

Encryption for Windows Devices. For devices running on a Windows operating system, dealers should strongly consider enabling BitLocker, which is Microsoft's free built-in mechanism for device encryption. For a collection of helpful articles on deploying BitLocker at your organization, see the following link: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

REQUIRED SERVICE PROVIDER CONTRACTS

APPLICABLE LAW OR REGULATION

16 CFR §314.4(f)(2)

Dealers must require that vendors with access to NPI sign a contract where they promise to implement reasonable safeguards.

Who needs to sign a GLBA Service Provider Addendum?

Any vendor who collects or processes NPI.

What if they refuse to sign?

While there is obviously no way to force vendors to sign the addendum, there are some actions you can take:

- Remind the service provider that they may be independently required to comply with the Revised Rule, so completing these items is mutually beneficial. Indeed, in a 2019 complaint against (and subsequent consent order with) a dealership DMS, the FTC took the position that businesses whose services facilitate financial operations on behalf of dealers are themselves considered financial institutions subject to the privacy and data security requirements under the GLBA Safeguards Rule.

- Determine if there's an existing contract with language that already satisfies the requirements of the Revised Rule. Ask your legal counsel to review your existing contract with the vendor as there may already be provisions that require the service provider to maintain appropriate safeguards. If the service provider refused to sign on this basis, ask them to produce a copy of the contract and cite to the applicable provision(s).

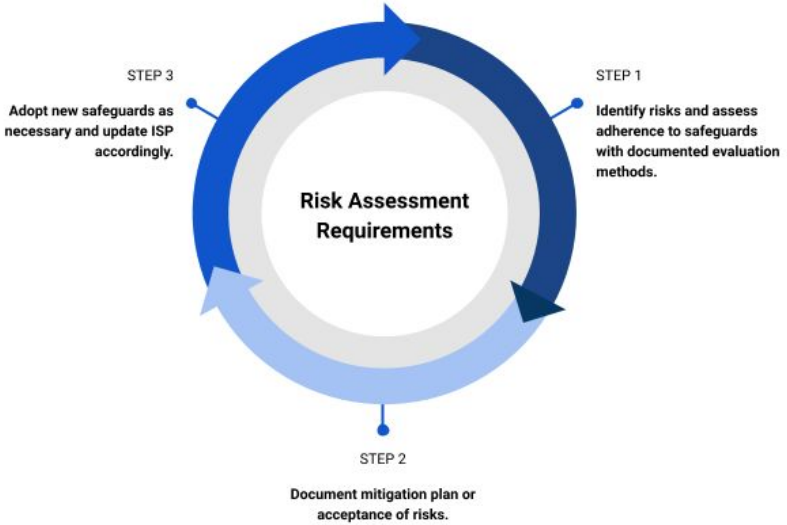
NJ CAR will be providing all attendees with a sample GLBA Service Provider Addendum

DOCUMENTED INTERNAL RISK ASSESSMENTS

APPLICABLE LAW OR REGULATION

16 CFR §314.4(b)

Dealers must have a written risk assessments for physical and technical safeguards that documents evaluation methods mitigation efforts.



Risk assessments should test for and incorporate, at a minimum, the following:

1. Safeguards required under the revised rule
2. Safeguards based on FTC enforcement actions
   - https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
3. Safeguards based on practices recommended by the FTC
   - https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

VENDOR RISK ASSESSMENTS

APPLICABLE LAW OR REGULATION

16 CFR §314.4(f)(3)

Dealers are required to periodically assess their service providers based on the risk they present and the continued adequacy of their safeguards.

Dealers must now assess the adequacy of their vendors' safeguards as well. Therefore, dealers should consider the following:

1. Before signing with a new service provider, require them to complete a risk assessment questionnaire that assesses their overall risk and ability to maintain appropriate physical, administrative, and technical safeguards; and

2. Require that existing service providers periodically complete a new risk assessment questionnaire as new risks or safeguards are identified.

NJ CAR will be providing all attendees with a sample vendor risk assessment questionnaire.

APPLICABLE LAW OR REGULATION

16 CFR §314.4(e)

Employees must be trained on security awareness and your information security program policies, procedures, and safeguards.

NEW EMPLOYEE TRAINING REQUIREMENTS

The Revised Rule now requires that dealers provide “security awareness training” to **all employees** as well as verifying that the information security personnel maintain current knowledge of changing information security threats and countermeasures.

NJ CAR and ComplyAuto have collaborated to provide the following online training course that adheres to the Revised Rule:

Dealership Security Awareness Course:
https://complyauto.com/security-awareness-course/

REQUIRED ANNUAL PENETRATION TESTING

APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(i)

Dealers must perform penetration tests of their IT infrastructure and information systems at least annually.

Penetration testing is a type of IT security test in which evaluators mimic real-world attacks to attempt to identify ways to circumvent the security features of an application, system, or network. A comprehensive internal penetration test will usually include, at a minimum, the following:

1. **Phishing and social engineering simulations**.
2. **Ransomware emulations**.
3. **Password cracking**.
4. **Credentials sniffing**.
5. **Web application attack simulations**.
6. **Active Directory attack simulations**.

⌘ TECHNOLOGY TIP

Phishing Simulations. A study by Verizon showed that 90% of ransomware and cybersecurity incidents involve clicking on a link in a phishing email. Consider using a phishing simulation software to test employees' security awareness and susceptibility to social engineering tactics. This normally involves sending out emails designed to look like real-life phishing emails, and then tracking which employees are willing to click on links within those emails or enter credentials on a fake landing page. “Phished” employees are then automatically enrolled in security awareness training. Internal phishing tests can be very effective at conditioning employees to scrutinize emails sent from people outside of your organization.

Penetration Testing. Many IT consulting firms and managed security service providers (MSSPs) offer internal penetration tests. Software is also available to help automate penetration testing without the need for evaluators to come on premises.

BIANNUAL VULNERABILITY ASSESSMENTS

APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(ii)

Dealers must perform vulnerability assessments at least biannually.

A vulnerability assessment is a scan of the entire IT environment in which all installed software is identified and checked for any publicly known security vulnerabilities.

Under the Revised Rule, vulnerability assessments must be performed once at least every six months.

⌘ TECHNOLOGY TIP

Open-Source Vulnerability Scanners. The FTC has mentioned OpenVAS, a free open source vulnerability scanner, as a tool that can be used to help satisfy the requirement for biannual vulnerability assessments. OpenVAS is a very popular tool for internal and external vulnerability scans. Vist https://www.openvas.org/ for more details. While not mentioned by the FTC, nMap is another popular open-source vulnerability scanner. Visit https://nmap.org/ for more details. However, dealers are advised to consult with experienced IT personnel before attempting to install and run these open source tools themselves.

OTHER REQUIREMENTS

- **Performing both a data and systems inventory**
  i. This requirement was designed to ensure that companies inventory the data in their possession and inventory the systems on which that data is collected, stored, or transmitted.
- **Annual written report to your Board of Directors or senior management.** Must include:
  i. The overall status of the ISP and compliance with the Revised Rule; and
  ii. Material matters related to the ISP, addressing issues such as risk assessments, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.
- **Implementing secure access controls**
  i. Includes technical controls, limitations on customer access to their own records, and physical controls

These requirements will be explained in more detail in the comprehensive compliance manual provided to attendees.

Interested in automating the complexities of the revised FTC Safeguards Rule with a purpose-built compliance solution?

Let ComplyAuto help ease the burden and cost of compliance.

SCHEDULE A DEMO

https://complyauto.com/schedule-demo/

TRANSPARENT PRODUCT PRICING

Single rooftop dealers: https://complyauto.com/pricing-single/

Dealer groups: https://complyauto.com/pricing-groups/

CONTACT US

chris@complyauto.com
CEO & Co-Founder
(385) 277-5882

https://www.complyauto.com

Facts

- The NADA estimated that the new rules would cost even small dealers *$276,925 per year*.
- Penalties for non-compliance are $43,792 per violation.
- ComplyAuto represents +750 dealers nationwide with a 100% client retention rate.
- ComplyAuto is a purpose-built solution by dealers, for dealers!