Complying with the Revised FTC Safeguards Rule

Dealer Compliance Manual

Last Revised: Dec 30, 2021

By ComplyAuto Privacy LLC

Chris Cleveland, CEO of ComplyAuto & Compliance Director of Galpin Motors
Hao Nguyen, General Counsel of ComplyAuto
https://www.complyauto.com

Overview

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. 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, 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.[1]

This Compliance Manual will cover the portions of the Revised Rule that are applicable to dealers and provide practical tips on how to achieve compliance.

Legal Disclaimer

This Compliance Manual is not intended as a source of legal advice nor a substitute for legal advice. Rather, this manual is intended to be a source of guidance for motor vehicle dealers on the revised FTC Safeguards Rule. The law is subject to constant change and there may have been developments since the date of this publication. Readers that require legal advice should contact competent counsel.

Copyright

About NJ CAR

NJ CAR advocates on behalf of New Jersey's $37B auto retail sector. The Coalition promotes public policies that ensure a fair and competitive marketplace, where the complex vehicle purchase process is made as simple and as seamless as possible.

New Jersey's extensive network of 500+ neighborhood new car dealers represents a fiercely competitive marketplace, which keeps motorists safe by ensuring ready access to warranty and safety recall service. It's fair to say that New Jersey new car dealerships are the economic engine on Main Street. They promote economic growth across the State by employing more than 39,000 people in great local jobs and investing millions of dollars in their communities.

[1] The penalty fee may be adjusted according to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015.

About the Authors

CHRIS CLEVELAND
Co-Founder & CEO, ComplyAuto
Compliance Director, Galpin Motors
chris@complyauto.com

Chris Cleveland is the Compliance Director of the Galpin Automotive Group and the Co-founder of ComplyAuto. He has spent over a decade specializing in automotive regulatory compliance and oversees a compliance team that conducts over 40 regularly scheduled audits in the areas of sales, finance, privacy, human resources, environmental health & safety, information security, and identity theft. In his role at ComplyAuto, Chris is committed to using his dealer experience to provide practical and automated software solutions that significantly reduce the dealership's potential liability with respect to government action and private lawsuits. He resides in Draper, Utah with his wife and son.

HAO NGUYEN
General Counsel, ComplyAuto
hao@complyauto.com

Hao Nguyen has spent his entire legal career in the automotive industry. After a stint with the California New Car Dealers Association (CNCDA), he joined Auto Advisory Services and helped in its transition to KPA after it was acquired in 2018. While there, he provided legal support in all functions at the dealership: from sales operation and registration to service department compliance and vehicle advertising. He now furthers the interests of automotive dealers in a different capacity and brings his knowledge and expertise to ComplyAuto, which is a cloud-based SaaS company offering a suite of solutions for complete dealership compliance. He resides in Long Beach, California with his wife and dog, Buster.

About ComplyAuto

Built by and for dealers, ComplyAuto is a software company specializing in automating privacy and cybersecurity compliance specifically for dealerships. ComplyAuto offers a full suite of solutions to achieve compliance with state and federal privacy and cybersecurity laws, like the revised GLBA Safeguards Rule and the state privacy laws. This includes penetration testing, vulnerability assessments, policy builders, data mapping, electronic risk assessments, vendor risk and contract management, and much more. Visit www.complyauto.com for more details.

Table of Contents

1. Summary of the Revised FTC Safeguards Rule

Effective Date

The Revised Rule goes into effect on January 10, 2022, though many of the requirements have been given a delayed effective date of December 9, 2022, as the FTC recognized the difficulty in achieving compliance with many of the technical requirements of the Revised Rule. The sections that require compliance by January 10, 2022 are as follows:

1. Performing periodic risk assessments.
2. Regularly testing or monitoring effectiveness of safeguards.
3. Overseeing service providers by (a) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards and (b) requiring specific contract terms.
4. Evaluating and adjusting the information security program in light of the results of the testing and monitoring.

Background

The Gramm-Leach-Bliley Act ("GLBA") is a federal law enacted in 1999 that was put in place to dictate how financial institutions protect the private information of individuals. It requires the Federal Trade Commission ("FTC") to implement regulations to carry out the GLBA's financial privacy provisions. The GLBA has three parts, but for the purposes of this writing, we will only concern ourselves with the Safeguards Rule, which was originally enacted in 2002 and recently revised on October 27, 2021.

The Safeguards Rule requires dealers to have measures in place to keep certain customer information secure and protected. Additionally, dealers must ensure that their affiliates and service providers safeguard the customer information in their care. With the significant rise of data breaches, cyberattacks, and ransomware across the country affecting many types of businesses, the FTC felt that it was their responsibility to bring the outdated Rule into the 21st century by introducing more specific requirements that dealers must abide by.

Dealers collect vast amounts of customer information in their daily operations and common interactions, including the financing and leasing of vehicles. The GLBA dictates what dealers must do to protect personally identifiable financial information. Some examples include:

- Formally creating and performing risk assessments in all aspects of dealer operations;
- Creating an information security program that lays out a plan to secure its databases within the organization;
- Conducting penetration testing and vulnerability scans;
- Developing security data disposal procedures to correctly (and legally) destroy customer information;
- Enacting basic access controls to strengthen employee logins and prevent security breaches; and

- Regularly testing or monitoring the effectiveness of key controls and implemented procedures

This may be a large and expensive undertaking for dealers of all sizes, particularly those who have not traditionally allocated resources to cybersecurity or data protection. When opposing the revision to the Rule, the National Automobile Dealers Association performed an analysis and opined that for a single dealership, compliance would require an average up-front cost of $293,975 and an average annual cost of $276,925 per year thereafter.[2]

Applicability to Dealers

Not only have dealers long been included on the list of businesses that must abide by the Rule, "automobile dealerships" are also specifically called out in the Revised Rule's definition of "financial institutions."[3] Similarly, the new exemptions listed in the Revised Rule are not likely to apply to dealers. For example, while financial institutions that maintain customer information of fewer than 5,000 consumers are exempt from certain requirements, it is highly unlikely that any dealer would fall under this exemption given the definition of "customer information" (which is defined below).

Definition of "Customer Information"

Per the Revised Rule, customer information under the GLBA is defined as "any record containing nonpublic personal information about a customer of a financial institution…that is handled or maintained by or on behalf of [the dealer] or [the dealer's] affiliates."[4] This includes:

1. Information a consumer provides in order to obtain a financial product or service;
2. Information about a consumer resulting from any transaction involving a financial product or service;
3. Any information obtained about a consumer in connection with providing a financial product or service; or
4. Any list, description, or other grouping or listing of consumers that is derived using such information.

For simplicity, this information will subsequently be referred to simply as "NPI" or "nonpublic personal information". Some common examples of NPI include customer information gathered as part of a leasing or financing transaction or a list of lease or finance customers used for advertising purposes.

While only NPI is covered by the Revised Rule, it is recommended that dealers treat any personally identifiable information (PII) they receive as part of the broader definition of "customer information" because of (1) the difficulty in determining the applicability of the Revised Rule in each particular context that information is collected, (2) the FTC's history of taking enforcement action against businesses who fail to reasonably protect information that falls outside the scope of NPI, and (3) the potential overlap with other state personal data laws and regulations. Therefore, unless otherwise

[2] Gilchrist, Charlie. "Proposed Safeguards Rule Changes Aren't the Right Path Forward for Dealers." *Official blog of NADA.* 23 Sept. 2019. https://blog.nada.org/2019/09/23/proposed-safeguards-rule-changes-arent-the-right-path-forward-for-dealers/ Accessed 12 Dec. 2021.
[3] 16 CFR § 314.2(h)(2)(ii)
[4] 16 CFR § 314.2(d)

noted, this Compliance Manual and Sample Information Security Program will treat both NPI and PII (hereinafter referred to collectively as "customer information") as covered under the Revised Rule.

Additional Proposed Changes to the Revised Rule

The Revised Safeguards Rule was published in the Federal Register on December 9, 2021, a date that starts the clock for financial institutions to implement certain requirements of the Revised Rule by specific deadlines (30 days or one year after the date of publication[5]). Along with this publication in the Federal Register, the FTC has opened a comment period to allow members of the general public to comment on its proposal to further amend the Safeguards Rule. Specifically, questions arise as to whether the financial institution must report to the FTC any "security event" where the financial institutions have determined misuse of customer information has occurred, or if it is likely that at least 1,000 consumers may have been affected. This comment period ends 60-days after the publication date. NJ CAR and ComplyAuto will be closely monitoring these additional proposed rules and will notify dealers and update this manual if they are adopted.

2. Appointing a Qualified Individual to Oversee Compliance

Under the Revised Rule, you must appoint a single "Qualified Individual" to oversee your Information Security Program ("ISP").[6] This individual is also known as the "Program Coordinator." 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. According to the FTC, dealers may designate any qualified individual who is appropriate for their business based on the business size and complexity.

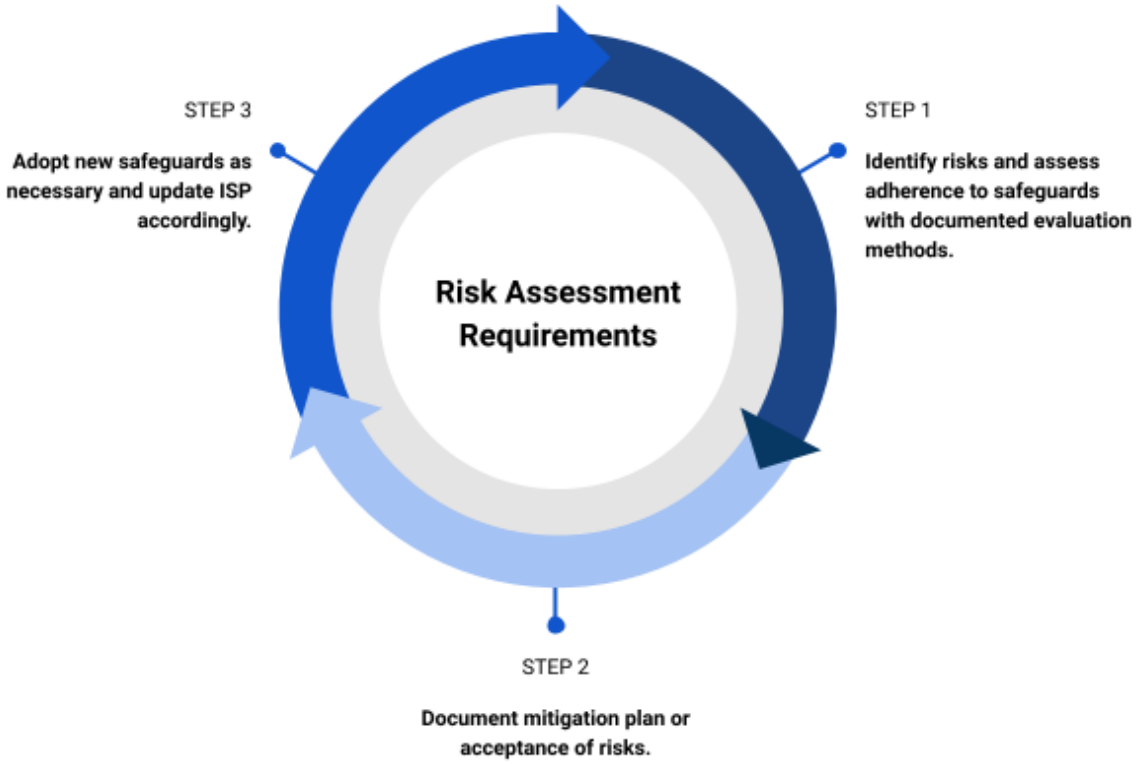
The purpose behind requiring designation of a single coordinator is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication. Unlike the original Safeguards Rule, the Revised Rule does not allow you to appoint multiple Program Coordinators. According to the FTC, splitting authority over an information security program between two or more people leads to failures of communications and oversight.[7]

Note that while the Program Coordinator must have ultimate responsibility for overseeing and managing the ISP, dealers may still assign particular duties, decisions, and responsibilities to other staff members. Moreover, the Revised Rule does not require that this be the Program Coordinator's sole job function – they may have other duties.

3. Completing Written Risk Assessments

[5] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272 (Dec. 9, 2021).
[6] 16 CFR § 314.4(a)
[7] *See e.g.*, Federal Trade Commission Staff Comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Oct. 24, 2019), at12-14 (suggesting that NIST clarify that one person should be in charge of the program). https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-preliminary-draft-nist-privacy-framework/p205400nistprivacyframeworkcomment.pdf. Accessed 13 Dec. 2021.

The Revised Rule requires that dealers perform written risk assessments that serve four general purposes: (1) identify potential physical, technical, and administrative security vulnerabilities and threats that may exist at their dealership, (2) include specific criteria that outlines methods on how the organization will mitigate those risks once they are identified (3) are performed periodically to reexamine potential risks, and (4) reassess the sufficiency and efficacy of any safeguards already in place to control those risks.[8] Finally, the required written ISP must be created and updated based on the results of these risk assessments. All of these requirements can be illustrated more simply in the following chart:



In performing their first risk assessments, dealers might start by evaluating and documenting adherence to the safeguards listed in Section 6 of the "Sample Information Security Program" provided at the end of this Compliance Manual.

4. Completing a Data and Systems Inventory

Under the Revised Rule, dealers are required to perform both a data and systems inventory. 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. According to the FTC,

[8] 16 CFR § 314.4(b)

this inventory forms the basis of an ISP because a system cannot be protected if the dealer does not understand its structure nor know what data is stored in which systems.[9]

A data and systems inventory is the process of identifying and tracking how customer information is collected and flows through the dealership (data mapping), as well as documenting where it is stored, who it is shared with, and for which business purposes it is collected. The dealership may have already performed at least part of this exercise to help comply with the CCPA and CPRA. Below is a sample of what conducting a data and systems inventory might look like:

Step 1: Identification of Data

Identify the categories of personal information collected in each department. Below is a sample list of personal information and department categories that may be used to start the data mapping process.

Categories of Personal Information	Departments
1. Identifiers 2. Customer Records Information 3. Characteristics of Protected Classifications under state and Federal Law 4. Commercial Information 5. Biometric Information 6. Internet or Other Electronic Network Activity Information 7. Geolocation Data 8. Audio, Video, Visual or Electronic Information 9. Professional or employment-related information 10. Education Information 11. Inferences drawn from categories above to create consumer preferences or behavioral profiles	1. Digital & Telemarketing 2. Sales and F&I 3. Service & Parts 4. Human Resources 5. Rentals & Loaners

Step 2: Identification of Sources & Business Purposes

After it is determined which categories of personal information are collected in each department, dealers should start identifying the categories of sources from which that information is collected and the business purposes for which it is used. Below is a sample list of sources and business purpose categories that serve as a good starting point.

Categories of Sources	Business Purposes
1. Directly from Consumers 2. Advertising Networks & Agencies 3. Data Brokers & Analytics Providers 4. Government Entities 5. Social Media Networks 6. Online Lead Providers	1. Auditing/Counting Ad Impression 2. Fraud/Security Incident Prevention 3. Contextual & Behavioral Targeting 4. Customer Service 5. Advertising & Marketing 6. Processing & Fulfilling Orders and

[9] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,286 (Dec. 9, 2021).

7. Credit Reporting Agencies 8. Vehicle Manufacturers 9. Captive Finance Companies 10. Vehicle Subscription Services 11. Insurance Companies 12. Internet Service Providers 13. Cell Phone Carriers 14. Tow Companies	Transactions 7. Providing Financing 8. Public Health & Safety Purposes 9. Defending Against Claims & Litigation

Step 3: Identification of Devices & Systems

Now that the dealership has identified the categories of personal information collected, the next step is to identify and document the devices and systems used to access or store customer information. Identifying *all* devices connected to the network is a critical part of this step so that no devices or systems accessing customer information get overlooked. Even prior to the Revised Rule, the FTC had taken enforcement action against companies for failing to inventory computers and devices connected to their network.[10] Given that dealers store most of their customer information in third-party vendor systems, a complete inventory of all vendors and service providers that have access to customer information must be completed. Below is a sample list of vendors that may have access to customer information:

[see next page for sample vendor list]

[10] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,286 (Dec. 9, 2021).

1. Appraisal Tools
2. Auctions & Wholesalers
3. Call Tracking & Phone Solutions
4. Car Rental Companies
5. Chat Modules
6. Check Guarantee Companies
7. Consumer Defense Attorneys
8. Credit Reporting & Compliance Systems
9. Credit Reporting Agencies (CRAs)
10. Customer Relations Management (CRM)
11. Data Analytics Tools
12. Dealer Management System (DMS)
13. Debt Collection Agencies & Repossession Companies
14. Desking Tools
15. Digital Retailers & eCommerce Platforms
16. Direct Mailers
17. DMV Title & Registration Software
18. Electronic Estimate & Invoice Tools
19. Electronic F&I Menu Systems
20. Email Blast Companies
21. F&I Product Providers & Administrators
22. Financial Institutions
23. Government Entities
24. Insurance Brokers
25. Lien Sale Companies
26. Online Service Appointment Schedulers
27. Parts eCommerce Platforms
28. Payment Processors & Gateways
29. Records Management Companies
30. Rental & Loaner Software
31. Repair & Sublet Facilities
32. Reputation Management Companies
33. Retargeting Services
34. Rideshare Companies
35. Sales and F&I Consultants
36. Service Communication Software
37. Service Department Consultants
38. Social Media Networks
39. Tax Accountants and Other Professionals
40. Text Messaging Tools
41. Tow Companies
42. Transportation Companies
43. Vehicle Manufacturers
44. Warranty Reimbursement Software or Services
45. Website Providers

⌘ TECHNOLOGY TIP

Data Inventories. Completing and managing a data inventory via a manual process with spreadsheets can be extremely challenging and time consuming. Therefore, dealers may want to consider the use of automated data mapping and vendor management software. Doing so allows dealers to more easily track and manage their vendors, as well as utilize interactive data maps to pinpoint exactly which categories of personal information are stored in which systems. The process is far more efficient and accurate.

Device & Systems Inventories. If the dealership has not been keeping track of the devices used across its network, it might seem like a daunting task to start doing so. However, the following is a list of free tools and software which can help to ease the burden of asset tracking:

- ***Nmap:*** Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to a network (https://nmap.org).
- ***Spiceworks:*** This is a free IT inventory and asset management software to identify devices and software on a network (https://www.spiceworks.com).
- ***CIS Hardware and Software Asset Tracking Spreadsheet:*** This free spreadsheet is created by CIS to help track enterprise systems and other assets. (https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-trackingspreadsheet/).

5. Encrypting of Data at Rest & In Transit

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).[11] Encryption is a complex topic that is outside the scope of this Compliance Manual, but dealers should start by considering encryption in the following contexts:

1. **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.

2. **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. A good practice relating to emails containing sensitive information is to send the information in a protected ZIP or RAR file, and then send the password to the file in a separate text, chat, or phone message.

3. **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!

4. **Third-Party Applications**. Dealers may have little control or insight into the encryption methodologies employed by their service providers. See Section 11 of this Compliance Manual for a discussion on assessing the adequacy of a service provider's physical, technical, and administrative safeguards. However, one thing dealers can control is how they are transmitting data to third parties. For example, transmitting sensitive customer information via a CSV file is not recommended. Instead, dealers should ask their service providers to provide a secure method of transmitting or uploading files containing customer information.

⌘ 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

[11] 16 CFR § 314.4(c)(3)

6. Implementing MFA for Systems Containing Customer Information

Multi-factor authentication ("MFA") is an authentication system that requires at least two distinct authentication factors for successfully logging into a system. The three authentication factors are:

1. Knowledge factors, such as a password;
2. Possession factors, such as an SMS/text or email token; and
3. Inherence factors, such as biometric characteristics, like a fingerprint.

Under the Revised Rule, dealers must require MFA for any system containing NPI.[12] 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.[13] There are three primary scenarios under which dealers will need to consider enabling MFA:

1. **Dealer's Internal Network & On-premise Applications**. Many dealerships self-host their own Dealership Management System ("DMS") and Customer Relations Management ("CRM") systems on their own internal networks or servers. Dealers may also have an on-premise document retention system for the electronic storage of deal jackets and repair orders. Some older software applications may run in the form of a desktop-based application that stores customer information locally on the machine. Finally, employees may download customer information directly onto their desktops or hard drives. In any of these cases, NPI may be stored on the dealers' own internal systems and therefore must be protected by MFA. In other words, when logging into their workstations (e.g., their Windows account), employees should be prompted for a possession factor such as an SMS/text or email token after successfully entering their password.

2. **Third-Party Web-based Applications**. Third party web-based applications containing NPI, such as the DMS and CRM, will need to be protected by MFA. Unfortunately, dealers might have little control over the functionality of the various cloud-based software they are using. Dealers will need to put pressure on their service providers to support MFA. The good news is that many popular software vendors, such as Dealertrack and RouteOne, already support MFA and account administrators will simply need to enable MFA in their security settings. While many other dealership software vendors have also announced their intent to support MFA because of the Revised Rule, dealers will undoubtedly face challenges getting each of their vendors to support MFA by the December 9, 2022 deadline.

3. **Remote Work**. In the wake of the COVID-19 pandemic, work from home has become increasingly common for dealership personnel. Any employee connecting remotely to the dealership's network should be required to use MFA due to the inherent heightened security risk.

[12] 16 CFR § 314.4(c)(5)
[13] Maynes, M. (March 2020). IT executives prioritize Multi-Factor Authentication in 2020. Retrieved Dec. 13, 2021, from https://www.microsoft.com/security/blog/2020/03/05/it-executives-prioritize-multi-factor-authentication-2020/.

⌘ **TECHNOLOGY TIP**

On-premises MFA. There are several popular software companies that offer solutions for on-premises multi-factor authentication, such as Okta and Duo Security. If dealers are storing NPI on their own internal devices, networks, or servers, 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.

🙋 **HR TIP**

Requiring MFA on Employee Cell Phones. Some state laws require that employers reimburse employees for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties. Employers that fail to do so can face wage and hour lawsuits. This is used commonly in the context of employees who are required to use their personal cell phone for work-related calls. One popular method of MFA is a text or SMS code that is sent to the user's cell phone. If your dealership is considering requiring this method of MFA for employee logins, please consult with competent legal counsel to discuss potential implications of your state's wage and hour laws.

7. Implementing Secure Access Controls

The Revised Rule requires that dealers implement secure access controls, which are defined as technical and physical controls designed to:

1. Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information.
2. Limit authorized users' access only to customer information that they need to perform their duties and functions.
3. In the case of customers, limit access to their own information.[14]

Regarding physical controls, the dealership should have a policy that limits the ability to request and access customer files (e.g., file rooms containing deal jackets and repair orders) to only authorized individuals on a need-to-know basis.

With respect to technical controls, the dealership should have a process for granting privileges for user accounts and systems containing personal information, such as in your CRM, DMS, credit-related systems, and document retention systems. Ideally, this includes "role-based access," which is a technique to define and manage access requirements for each account based on need to know, level of privilege, and separation of duties. For example, if electronic deal jackets are bundled

[14] 16 CFR § 314.4(c)(1)

into one file folder that cannot be segmented for access purposes, consider breaking up each electronic deal file into folders based on need-to-know access principles. For instance, a Service Manager probably doesn't need access to credit applications. To prevent the Service Manager from accessing information that they do not need to, the dealership might have separate "credit" and "service contracts" folders so that Finance Managers can access the former while Service Managers can access only the latter. Finally, only a few select individuals should have administrative access to these systems and all administrative access should be centralized in a neutral department, such as IT, so they can better enforce and manage granting and revoking access to sensitive systems.

Regarding limits on customers accessing their own files, consider implementing a customer records request policy, such as the sample listed in Section 6.5 of the "Sample Information Security Program" at the end of this Compliance Manual.

8. Conducting Annual Penetration Tests

The Revised Rule requires that dealers perform internal penetration tests at least annually.[15] 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. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual hackers. The goal of this exercise is to expose vulnerabilities so that the organization can work to reinforce their data security protocols. While the Revised Rule does not specifically state what a penetration test must include, a comprehensive internal penetration test will usually include, at a minimum, the following:

1. **Phishing and social engineering simulations**. Phishing is a technique for attempting to acquire sensitive data, such as account credentials, through a fraudulent solicitation in an email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Users are also tricked into downloading a malicious file which can then be used for ransomware or other attacks. In the publication containing the final Revised Rule, the FTC clarified that internal social engineering and phishing campaigns are an important part of the penetration testing requirement.[16]

2. **Ransomware emulations**. Ransomware is an increasingly popular form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. These malicious actors will then demand money in exchange for an encryption key that can be used to unlock your files (though the key may not always work). Many ransomware attackers will also extort businesses by threatening to publish sensitive information publicly online. Ransomware emulations execute end-to-end attack flows of the most notorious ransomware campaigns to validate readiness of an organization's network for a real ransomware attack.

3. **Password cracking**. Just like it sounds, password cracking is the process of recovering protected passwords stored in a computer system or transmitted over a network. This is an

[15] 16 CFR § 314.4(d)(2)
[16] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,277 (Dec. 9, 2021).

attack that is often done if attackers are able to access your stored, encrypted passwords (e.g. stored in Windows Active Directory) and want to recover the original, plain-text password. A full internal penetration test will normally run password cracking tools designed to test the strength of password policies across your dealership's network and devices.

4. **Credentials sniffing**. Credentials sniffing is a technique used by hackers to monitor web and network traffic for plaintext or exposed user credentials. Penetration tests will normally run tools that "sniff out" such credentials through publicly known vulnerabilities.

5. **Web application attack simulations**. Web-based applications have become primary targets of attacks. This includes attacks such as buffer overflows, cross-site scripting (XSS), and SQL injection vulnerabilities. An internal penetration test will normally run these types of simulated attacks across your web-based applications, such as a dealership's internal intranet and self-hosted websites. Most dealerships rely on third-party website providers, in which case you should refer to Section 10 of this Compliance Manual discussing requirements to assess your service providers.

6. **Active Directory attack simulations**. In a Microsoft Windows or Active Directory environment (which is used by many dealerships), there is a hacking technique known as "Kerberoasting" that takes advantage of the Windows Kerberos' Ticket Granting service and can be used to obtain hashed credentials that attackers attempt to crack. A full internal penetration test will normally attempt to simulate this attack vector in order to identify vulnerabilities.

⌘ 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.[17] 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.

[17] Schwartz, M. J. (March 2017). Verizon: Most Breaches Trace to Phishing, Social Engineering. Retrieved on Dec. 14, 2021, from https://www.bankinfosecurity.com/interviews/verizon-most-breaches-trace-to-phishing-social-engineering-i-3516.

9. Conducting Biannual Vulnerability Assessments

A vulnerability assessment is any systemic scan or review of a dealership's network and information systems that is designed to identify known security vulnerabilities. Put in simpler terms, it's 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.[18]

The FTC has indicated that free automated vulnerability scanning tools can be used to satisfy this requirement.[19] However, dealers choosing to use free or open-source vulnerability scanning tools are cautioned that they will likely need to have experts on staff to understand the results that the scanning tools produce, how to identify false positives, how to manage identified vulnerabilities, and how to fix them. Even installing such tools can be difficult without the requisite technical expertise.

⌘ 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.[20] 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, as mentioned above, dealers are advised to consult with experienced IT personnel before attempting to install and run these open source tools themselves.

10. Assessing Adequacy of Service Provider Safeguards

For service providers that have access to NPI, dealers are required by the Revised Rule to do the following[21]:

1. Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the NPI at issue;
2. Require the service providers, by contract, to implement and maintain such safeguards; and
3. Periodically assess the service providers based on the risk they present and the continued adequacy of their safeguards.

In order to accomplish the above requirements, dealers should consider implementing the following:

[18] 16 CFR § 314.4(d)(2)
[19] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,280 (Dec. 9, 2021).
[20] For the Record, Inc., Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule. July 2020. 140:6-16. Retrieved Dec. 13, 2021 from https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf.
[21] 16 CFR § 314.4(f)

1. Have all service providers that collect NPI sign a GLBA Safeguards Addendum that requires them, by contract, to maintain appropriate safeguards;
2. 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
3. Require that existing service providers periodically complete a new risk assessment questionnaire as new risks or safeguards are identified.

Given the Revised Rule's new requirements for encryption and MFA (see Sections 5 & 6 of this Compliance Manual), dealers should reconsider onboarding or continuing to use service providers that are not willing to represent support of those security features. Some service providers may refuse to complete a risk assessment questionnaire or GLBA Service Provider Addendum. While there is obviously no way to force vendors to complete these items, 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.[22]
- 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).
- As an alternative to a risk assessment questionnaire, ask the service provider to produce a copy of a report certifying compliance with an industry standard cybersecurity framework, such as ISO 27001, NIST, or CIS Controls.

To better serve dealer members, NJ CAR and ComplyAuto have worked together to create the following sample GLBA Service Provider Addendum and Risk Assessment Questionnaire. Of course, dealers should work with legal counsel to ensure these items are customized to meet the needs of their dealerships and service providers.

Note that while the CCPA and CPRA also require that service providers sign a data processing agreement that contains certain representations, both the definition of what constitutes a "service provider" and the required representations are much different under the GLBA. The key difference is that any vendor collecting or processing **PII** should be required to sign a CCPA/CPRA service provider addendum, while only vendors collecting **NPI** are required to sign the GLBA Service Provider Addendum shown below. Additionally, some vendors who collect both PII and NPI may need to sign both addenda. Please reference the NJ CAR's CCPA Handbook for more details on the CCPA's service provider requirements.

[22] *In the Matter of LightYear Dealer Technologies, LLC.*, No. C-4687. FTC Complaint. Retrieved on Dec. 13, 2021 from https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_final_complaint.pdf

Sample GLBA Service Provider Addendum

This Addendum is between _____(hereinafter referred to as "Service Provider") and _____and/or any of its affiliated entities for which Service Provider either (1) seeks to enter into a business relationship with, or (2) has an existing business relationship with (hereinafter collectively referred to as "Dealer"). The federal Gramm-Leach-Bliley Act (GLBA) "Safeguards Rule" requires that Service Providers who are permitted access to Dealer's "Customer Information" enter into an agreement whereby the Service Provider promises to implement and maintain appropriate safeguards designed to protect the Customer Information at issue. This Addendum supplements and amends any and all agreements between Service Provider and Dealer and constitutes a Service Provider agreement subject to the GLBA Safeguards Rule. To the extent there is any ambiguity or conflict between any other agreement and this Addendum, the terms of this Addendum shall apply. It shall be effective as of the date the document is executed below by Service Provider. If any provision of this Addendum is found invalid or unenforceable, all remaining provisions of this Addendum will remain in full force and effect. This Addendum shall remain in effect until either revoked in writing or automatically if the business relationship between Dealer and Service Provider comes to an end, except that the representations and warranties listed in Section 2 of this agreement shall survive any termination.

1. **Customer Information**. As the term is defined in the GLBA Safeguards Rule (16 C.F.R. § 314.2), "Customer Information" means any nonpublic personal information (i.e., personal financial information or information derived from nonpublic financial information) collected by Dealer about its customers, including:

a. Information a consumer provides in order to obtain a financial product or service;
b. Information about a consumer resulting from any transaction involving a financial product or service;
c. Any information otherwise obtained about a consumer in connection with providing a financial product or service;
d. Any list, description, or other grouping of consumers that is derived using the information described in items 1.a. through 1.c. above.

2. **Service Provider Representations & Warranties**. With the mutual goal of maintaining proper protocols to protect customer information, Service Provider represents and warrants that:

a. It will not disclose or use Customer Information other than to carry out the purposes for which Dealer disclosed the information pursuant to its contractual agreement with Service Provider (the "Services");
b. It maintains Customer Information only for as long as necessary to provide the Services;
c. It will return or securely destroy all Customer Information received from Dealer upon either completion or termination of the Services;
d. It is capable of implementing and meeting all local, state, and federal legal requirements regarding the required administrative, technical, and physical safeguards under those laws,

and all applicable industry standards with respect to the privacy and security of the Consumer Information that it maintains, processes, obtains, or otherwise has access to; and

e. It will protect and secure any Customer Information that it maintains, processes, obtains, or otherwise has access to as required under all applicable local, state, and federal privacy data and security laws and regulations.

3. **Risk Assessments**. Service Provider will, upon Dealer's request, complete a questionnaire that assesses Service Provider's ability to comply with Section 2.d. and 2.e. above.

4. **Breach & Termination**. Notwithstanding anything to the contrary in any other agreement, Service Provider's violation of any terms of this Addendum shall be deemed a material breach and Dealer may immediately terminate its relationship with Service Provider without penalty. Dealer may seek injunctive relief, in addition to a claim for damages, in order to prevent or remedy any breach of the obligations of this Addendum.

_____
Date

_____
Signature of Authorized Agent of Service Provider

_____
Printed Name and Title

Sample Risk Assessment Questionnaire for Service Providers

Physical and Administrative Questions

1. Does your company have a written information security program?

○Yes ○No ○N/A

2. Does your company perform physical, administrative, and electronic risk assessments relating to information safeguards at least annually?

○Yes ○No ○N/A

3. Does your company perform training on security awareness for all employees at least annually?

○Yes ○No ○N/A

4. Does your company have a cybersecurity insurance policy that covers data breaches affecting customer personal information that you collect, receive, store, or process on our behalf?

○Yes ○No ○N/A

5. Does your company have a process and/or policy that limits the ability to request and access files (whether stored physically or electronically) containing customer information to only authorized individuals with a need-to-know basis?

○Yes ○No ○N/A

6. Does your company provide a mechanism for the secure destruction and disposal of documents containing personal information, such as locked shredding bins?

○Yes ○No ○N/A

7. Does your company ask that each of your service providers and sub-processors sign a data processing agreement that complies with applicable state and federal data privacy laws?

○Yes ○No ○N/A

8. Does your company use and share only fictitious or test data (not real customer information) for training, development, or testing purposes?

○Yes ○No ○N/A

9. Has your company experienced a data breach affecting consumer personal information in the past 12 months?

○Yes ○No ○N/A

Electronic & Technical Questions

1. Does your company conduct social engineering and phishing simulations?

○Yes ○No ○N/A

2. If your company offers a software or application as part of its services, does it support multi-factor authentication, such as SMS or email tokens?

○Yes ○No ○N/A

3. Has your company performed a full penetration test in the last 12 months?

○Yes ○No ○N/A

4. Does your company regularly run internal and external vulnerability scans or have a system for continuous monitoring of threats?

○Yes ○No ○N/A

5. Does your company store network user credentials securely by ensuring such credentials are not stored in plain, readable text or in a vulnerable format?

○Yes ○No ○N/A

6. Does your company restrict access to sensitive data stored in files and on your network and ensure that only authorized employees with a business need have access to personal information?

○Yes ○No ○N/A

7. If your company offers a software or application as part of its services, does it require the use of complex and unique passwords (alpha-numeric and non-dictionary words) for all systems containing personal information?

○Yes ○No ○N/A

8. If your company offers a software or application as part of its services, does it protect against brute-force attacks by suspending or disabling user credentials after a certain number of unsuccessful login attempts?

○Yes ○No ○N/A

9. If your company offers a software or application as part of its services, does it use properly configured and industry-tested methods of encryption to keep sensitive information secure in transit and at rest?

○Yes ○No ○N/A

10. If your company offers a software or application as part of its services, do you (1) employ engineers trained in secure coding, (2) test for common vulnerabilities, (3) follow platform and OS guidelines for security, and (4) verify that privacy and security features work as intended?

○Yes ○No ○N/A

11. Does your company regularly update and patch third-party software (e.g., antivirus, firewalls) and test your network to ensure that such updates and patches have been successfully installed on all applicable devices?

○Yes ○No ○N/A

11. Implementing a Written ISP & Other Policies

The Revised Rule requires that dealers implement a series of written policies and procedures. A sample Information Security Program ("ISP") that includes each of the following policies and procedures is included at the end of this Compliance Manual.

1. **Information Security Program**. While dealers have been required to have a written ISP since the original Safeguards Rule was enacted in 2002, the program must be updated to meet a host of new requirements under the Revised Rule.[23]

2. **Incident Response Plan**. The Revised Rule requires a documented incident response plan that addresses the following areas[24]:
    a. The goals of the incident response plan;
    b. The internal processes for responding to a security event;
    c. The definition of clear roles, responsibilities, and levels of decision-making authority;
    d. External and internal communications and information sharing;
    e. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
    f. Documentation and reporting regarding security events and related incident response activities; and
    g. The evaluation and revision as necessary of the incident response plan following a security event.

3. **Data Retention Policy**. This is a new requirement that requires that dealers adhere to a written data retention policy in order to minimize the unnecessary retention of customer information. The policy must include a record retention schedule and procedures for the secure disposal of customer information, in any format, no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is[25]:
    a. necessary for business operations or for other legitimate business purposes;
    b. otherwise required to be retained by law or regulation; or
    c. not reasonably feasible due to the manner in which the information is maintained.

4. **IT Change Management Procedures**. This is a new requirement that requires dealers to have written procedures in place with respect to adding, removing, or modifying any part of their IT infrastructure.[26] The reason for this requirement is that changes to an organization's network, servers, devices or information systems may open new vulnerabilities or introduce a heightened risk of cybersecurity incidents.

[23] 16 CFR § 314.4(b)
[24] 16 CFR § 314.4(h)
[25] 16 CFR § 314.4(c)(6)
[26] 16 CFR § 314.4(c)(7)

12. Reporting on the Status of your ISP to the Board

The Revised Rule requires that the single "qualified individual" (described in Section 2 of this Compliance Manual) report in writing, at least annually, to the dealership's board of directors or equivalent governing body.[27] If no such board of directors or equivalent governing body exists, such reports shall be timely presented to a senior officer responsible for the dealer's information security program. However, even if a senior officer is appointed as the qualified individual, that person must still report the results of the ISP to some other senior officer or governing body. The written report must include the following information:

1. The overall status of the ISP and compliance with the Revised Rule; and
2. 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.

According to the FTC, this new requirement is intended to do the following[28]:

1. Ensure the dealership's governing body (such as a board of directors or senior officer) is engaged with and informed about the state of the dealer's ISP;
2. Create accountability for the single "qualified individual" by requiring them to set forth the status of the information security program for the board or senior officer;
3. Help dealers ensure their ISP is being maintained appropriately and given the necessary resources;
4. Create a record of decisions made and the information upon which they were based, which may aid future decision-making; and
5. Encourage management involvement in the ISP to improve the strength of those programs and help reduce breaches.

13. Implementing a Security Awareness Training Program

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.[29] While the Revised Rule does not specify the content of this training, dealers might consider looking to internationally accepted cybersecurity frameworks for guidance, such as the Center for Internet Security Critical Security Controls ("CIS Controls"). The CIS Controls require that companies maintain a security awareness training program that includes the following subject matter:

1. The dangers of connecting to, and transmitting data over, insecure networks for enterprise activities;

[27] 16 CFR § 314.4(i)
[28] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,299 (Dec. 9, 2021).
[29] 16 CFR § 314.4(e)(1)

2. Understanding how to verify and report out-of-date software patches or any failures in automated processes and tools;
3. Recognizing a potential incident and reporting such an incident;
4. Causes for unintentional data exposure;
5. How to identify and properly store, transfer, archive, and destroy sensitive data;
6. Authentication best practices; and
7. Recognizing social engineering attacks, such as phishing, pretexting, and tailgating.

NJ CAR and ComplyAuto have collaborated to provide the following online training course that adheres to both the Revised Rule and CIS Controls to all NJ CAR members:

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

14. Using Software to Comply with the Revised Safeguards Rule

As stated earlier, the FTC revised the Safeguards Rule knowing full well about the technological capabilities that businesses currently have at their disposal. In fact, in its 145-page commentary answering many concerns businesses brought forward regarding the potential cost and complexity, the FTC frequently cited to the availability of resources to help businesses comply with these new requirements.

Dealers should consider using an outside vendor to help them navigate through these requirements, especially if they do not have the resources to do this on their own. Much like how the Safeguards Rule itself was outdated in its prior iteration in the early 2000s, compliance has, in some ways, outgrown the manual processes that were sufficient at the time. Not even considering the convenience of technology, software is arguably required in the following instances:

- Electronic penetration testing of dealership defensive protocols;
- Vulnerability scans of dealer databases;
- Phishing simulation and other social engineering campaigns to train employees on ransomware and data breach; and
- Data inventory and mapping to identify customer information and third-party vendors.

The use of automation and software to meet the existing and new requirements of the Revised Rule is almost a necessity if dealers want to comply without heavily disrupting daily operations. A good vendor in this space will know how dealerships work and possess both the legal and technical expertise to help. Relative to a typical financial institution, a dealership operates on a different plane while having to fulfill the same complex requirements. Using industry-specific knowledge, the vendor should know the kinds of customer information a dealer collects in the many different interactions a customer could have at the store and the types of third-party vendors that would have access to this information.

15. Sample Information Security Program

The following ISP is a collection of sample policies that can be used by dealerships as a starting point to satisfy the following requirements of the Revised Rule. It consists of the following:

1. Written Information Security Program;
2. Written incident response plan;
3. Written IT change management procedures; and
4. Written data retention plan and disposal procedures

We caution against using the sample documents below without consulting with competent legal counsel to customize the documents as necessary to reflect the dealership's actual cybersecurity practices and needs. For the section with checkboxes for individual safeguards, any safeguards not implemented by the dealership should be removed. Similarly, if the dealership is not following the CIS Controls, that section should be removed.

Note that the Sample ISP below has intentionally included a broader definition of customer information than required by the Revised Rule due to (1) the difficulty in determining the applicability of the Revised Rule in each particular context that information is collected, (2) the FTC's history of taking enforcement action against businesses who fail to reasonably protect information that falls outside the scope of NPI, and (3) the potential overlap with other state personal data laws and regulations.

[see next page for sample Information Security Program]

[Dealership_Name] Information Security Program

[LastUpdatedDate]

1. Scope & Objectives

The objectives of this comprehensive written Information Security Program ("**ISP**") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards [Dealership_Name] has selected to protect the personal information it collects, receives, uses, and maintains. All employees, staff, contractors, and guests of the following locations are expected to comply with this ISP:

[Dealership_Locations]

All locations shall protect customer information by adopting and implementing, at a minimum, the security standards, policies, and procedures outlined in this ISP. This ISP outlines the minimum standards for the protection of personal information and each location is encouraged to adopt standards that exceed the requirements outlined in this ISP. This ISP has been developed in accordance with the requirements of all applicable state and federal laws, including, but not limited to, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. §§ 314.1 to 314.5). If this ISP conflicts with any legal obligation or other [Dealership_Name] policy or procedure, the provisions of this ISP shall govern.

The purpose of this ISP is to:

1. Ensure the security, confidentiality, integrity, and availability of personal information [Dealership_Name] collects, receives, uses, and maintains.
2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
3. Protect against unauthorized access to or use of [Dealership_Name]-maintained personal information that could result in substantial harm or inconvenience to any customer or employee. Fulfill [Dealership_Name]'s obligation to comply with all state and federal regulations, policies, and standards associated with safeguarding customer information.
4. Define an information security program that is appropriate to [Dealership_Name]'s size, scope, and business, its available resources, and the amount of personal information that [Dealership_Name] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

This ISP applies to all employees, contractors, officers, and directors of [Dealership_Name]. It applies to any records that contain personal information in any format and on any media, whether in electronic or paper form.

For purposes of this ISP, "**personal information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer:

1. Identifiers such as a real name, alias, postal address, online identifiers such as Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
2. Customer records, including but not limited to, digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).
3. Characteristics of protected classifications under state or federal law.
4. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. Biometric information.
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
7. Geolocation data.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99).
11. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
12. Persistent identifiers that can be used to recognize a consumer or a device that is linked to a consumer, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

"Personal information" does not include publicly available information, aggregate consumer information, or consumer information that is deidentified. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records.

2. Program Coordinator

This ISP and the safeguards it contemplates are implemented and maintained by a single qualified employee or service provider ("Program Coordinator") designated by [Dealership_Name]. The Program Coordinator is responsible for the design, implementation, and maintenance of information safeguards and other responsibilities as outlined in this ISP. The Program Coordinator may delegate or outsource the performance of any function under the ISP as he or she deems necessary from time to time. [Dealership_Name] has designated the following individual as the Program Coordinator:

[Program_Coordinator_Contact_Info]

The Program Coordinator shall be responsible for the following:

- Implementation and maintenance of this ISP, including, but not limited to:
    - Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation steps;
    - Coordinating the development, distribution, and maintenance of information security policies and procedures;
    - Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information;
    - Ensuring that the safeguards are implemented and maintained to protect personal information throughout [Dealership_Name], where applicable;
    - Overseeing service providers, processors, and third parties that access or maintain personal information on behalf of [Dealership_Name];
    - Monitoring and testing the ISP's implementation and effectiveness on an ongoing basis through documented risk assessments and other mechanisms;
    - Defining and managing incident response procedures; and
    - Establishing and managing enforcement policies and procedures for this ISP, in collaboration with [Dealership_Name]'s legal counsel, human resources department, and upper management.
- Employee, staff, and contractor information security training, including:
    - Providing periodic security awareness and related training regarding this ISP, [Dealership_Name]'s safeguards, and relevant information security policies and procedures for all employees, staff, and contractors;
    - Ensuring that those employees, staff, and contractors who have been enrolled in training courses have completed and passed the course in a timely manner; and
    - Retaining training completion records.
- Reviewing this ISP at least annually, or whenever there is a material change in [Dealership_Name]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information.
- Periodically reporting to [Dealership_Name] management regarding the status of the information security program and [Dealership_Name]'s safeguards to protect personal information.

3. Implementation Cycle

[Dealership_Name] utilizes a methodology that establishes information security policies based on periodic and updated risk assessments. Once initial risks are identified and assessed, mitigation controls are documented by the Program Coordinator or his/her designees. Employees are then trained and made aware of their responsibilities for following the proper information safeguards outlined in this document. Each [Dealership_Name] location will then be monitored and tested for its effectiveness at complying with the safeguards by performing updated risk assessments, performed at least annually. The process continues as periodic audits and risk assessments are conducted to identify and evaluate residual risk.

4. Risk Assessments

As a part of developing and implementing this ISP, [Dealership_Name], for each location, will conduct and document periodic risk assessments, at least annually, or whenever there is a material change in [Dealership_Name]'s business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

The risk assessment shall evaluate:

1. Reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information;
2. The likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information; and
3. The sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
    a. Employee, staff, and contractor training and management;
    b. Employee, staff, contractor, service provider, process, and third-party compliance with this ISP and related policies and procedures;
    c. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
    d. [Dealership_Name]'s ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, [Dealership_Name] will:

1. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
2. Make available the results of the risk assessment to upper management for review;
3. Reasonably and appropriately mitigate any identified risks or violations of this ISP and document such mitigation in the risk assessment; and
4. Regularly monitor the effectiveness of [Dealership_Name]'s safeguards, as specified in this ISP.

5. Safeguard Principals

[Dealership_Name] will develop, implement, and maintain reasonable administrative, electronic, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that [Dealership_Name] owns, accesses, or maintains on behalf of others. In doing so, [Dealership_Name] will adhere to the following principles:

1. Safeguards shall be appropriate to [Dealership_Name]'s size, scope, and business, its available resources, and the amount of personal information that [Dealership_Name] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee personal information.
2. [Dealership_Name] shall document its administrative, electronic, technical, and physical safeguards (see Section 6 of this ISP).
3. [Dealership_Name]'s administrative safeguards shall include, at a minimum:
    a. Designating one or more employees to coordinate the information security program (see Section 2 of this ISP);
    b. Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 3 and 4 of this ISP);
    c. Training employees in security program practices and procedures (with management oversight);
    d. Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7 of this ISP); and
    e. Adjusting the information security program in light of business changes or new circumstances.
4. [Dealership_Name]'s electronic and technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, support:
    a. Secure user authentication protocols, including:
        i. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
        ii. Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
        iii. Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
    b. Secure access control measures, including:
        i. Restricting access to records and files containing personal information to those with a need-to-know to perform their duties; and

ii. Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

c. Encryption of all personal information traveling wirelessly or across public networks;
d. Encryption of all personal information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal information stored on any other device or media (data-at-rest);
e. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures;
f. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information; and
g. Current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

5. [Dealership_Name]'s physical safeguards shall, at a minimum, provide for:
   a. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers;
   b. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal; and
   c. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

6. Information Security Policies, Procedures & Safeguards

The following policies, procedures, and safeguards reflect [Dealership_Name]'s objectives for managing operations and controlling activities related to information security. Additionally, the policies and procedures within this document represent [Dealership_Name]'s ongoing efforts in achieving and maintaining internal control over customer information security as well as compliance with state and federal requirements. This section of the ISP outlines minimum requirements and is not meant to be a comprehensive or all-inclusive list. The Program Coordinator shall implement, test, monitor, and enforce all of the policies and procedures covered below:

1. General Dealership Safeguards

a. Documents with personal information shall not be left unattended on the desk or workspace of any employee. At a minimum, employees shall place any documents containing customer information in a drawer or enclosed container.

b. Customer personal information that is no longer part of an ongoing transaction (e.g., "dead" or "lost" deal documentation) should generally not be retained unless required by law or [Dealership_Name] policy, or unless it is securely stored, such as in a locked drawer or file cabinet.
c. When away from their office, desk, or workspace, employees, staff, and contractors shall either (1) lock their office doors, or (2) utilize lockable storage for any customer personal information. If keys and/or locks are not available, then the workspace shall be cleared of all customer personal information, with no customer personal information left visibly unattended.
d. Files and documents containing personal information that do not need to be retained by state, federal, or internal [Dealership_Name] rules shall be securely destroyed and never placed into a regular trash or recycling bin. This includes mistakenly printed documents (including duplicates), as well as handwritten notes with customer personal information such as names, addresses, emails, and telephone numbers.
e. Printers, fax machines, copiers, and other office equipment shall be located in secure areas that are well monitored. At a minimum, documents should be immediately retrieved when faxed or printed from a remotely located machine. Under no circumstances should a document be left unattended at an unsecured machine location. Trash bins near copiers, printers, and other office equipment should be inspected for documents containing personal information.
f. Personal information should never be placed in a manner that exposes customer information to unintended individuals. When with a customer, only that customer's personal information should be visible near the employee's desk or workspace.
g. Credit application interviews, as well any other verbally communicated information involving the collection or disclosure of personal information, shall be conducted in areas secure from eavesdropping. Employees shall not use speakerphones in open areas susceptible to eavesdropping.
h. All new employees should be trained on the basics of customer information security policies, procedures and safeguards outlined in this ISP. This should be conducted during, and incorporated into, the new employee onboarding process. Training shall recur, at a minimum, annually for each employee.
i. All employees shall be granted access to customer information (both physical and electronic) on a need-to-know and least-access basis.
j. [Dealership_Name] shall conduct an inventory of all categories of personal information collected, map to which departments it is shared, the business purposes for which it is shared or disclosed, the categories of third parties and service providers to whom it is shared or disclosed, and the categories of sources from whom it is collected.

2. Physical & Administrative Safeguards

a. [Dealership_Name] recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the physical and administrative

safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, [Dealership_Name] shall do each of the following (check all that apply):

- ☐ Limit Access to Customer Files to Individuals with a Need-to-Know
- ☐ Protect File Storage Areas with Locking or Continuous Monitoring
- ☐ Ensure Copiers and Office Equipment Are Kept Clear of Personal Information
- ☐ Protect File Storage Areas from Destruction and Damage
- ☐ Ensure Unattended Computers Are Not Left Unlocked
- ☐ Ensure Proper Disposal of Customer Information
- ☐ Provide Mechanisms for Secure Disposal of Personal Information
- ☐ Ensure Unattended Workspaces Are Kept Clear of Personal Information & Security Credentials
- ☐ Keep Safety Standards in Place when Data is En Route
- ☐ Require locking unattended offices and cabinets containing customer information

3. **Electronic & Technical Safeguards**
    a. [Dealership_Name] recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the technical safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, [Dealership_Name] shall do each of the following (check all that apply):

- ☐ Hold On to Information Only as Long as You Have a Legitimate Business Need
- ☐ Use Only Fake or Test Data for Training and Testing Purposes
- ☐ Restrict Electronic Access to Sensitive Data to Individuals With a Business Need
- ☐ Limit Administrative Access to a Neutral Department or Person
- ☐ Require Complex and Unique Passwords
- ☐ Ensure User Credentials Are Not Stored in Vulnerable Formats
- ☐ Enable MFA for All Systems Containing Non-public Personal Information
- ☐ Disable User Accounts After Multiple Unsuccessful Login Attempts
- ☐ Encrypt Data at Rest and in Transit
- ☐ Use Firewalls to Segment Networks
- ☐ Use or Enable Intrusion Detection and Monitoring Tools
- ☐ Require Remote Network Access Be Done Through VPN and MFA
- ☐ Place Limits on Third-Party Access to Networks and Applications
- ☐ Update and Patch Third-Party Software
- ☐ Encrypt Data Sent Over Point-of-Sale Devices
- ☐ Restrict Downloading of Unauthorized Software
- ☐ Encrypt Information Sent Over Wireless Networks
- ☐ Ensure Digital Copiers Have Encryption or Overwriting Enabled
- ☐ Add Auto-Wiping, Encryption, or Centralized Computing to Mobile Devices

4. Adoption of Safeguards under the CIS Controls Framework

a. [Dealership_Name] also adopts the physical, administrative, and technical safeguards outlined in version 8 of the Center for Internet Security (CIS) Controls. Accordingly, [Dealership_Name] shall do each of the following (check all that apply):

- ☐ Establish and Maintain Detailed Enterprise Asset Inventory
- ☐ Address Unauthorized Assets
- ☐ Establish and Maintain a Software Inventory
- ☐ Ensure Authorized Software is Currently Supported
- ☐ Address Unauthorized Software
- ☐ Establish and Maintain a Data Management Process
- ☐ Establish and Maintain a Data Inventory
- ☐ Configure Data Access Control Lists
- ☐ Enforce Data Retention
- ☐ Securely Dispose of Data
- ☐ Encrypt Data on End-User Devices
- ☐ Establish and Maintain a Secure Configuration Process
- ☐ Establish and Maintain a Secure Configuration Process for Network Infrastructure
- ☐ Configure Automatic Session Locking on Enterprise Assets
- ☐ Implement and Manage a Firewall on Servers
- ☐ Implement and Manage a Firewall on End-User Devices
- ☐ Securely Manage Enterprise Assets and Software
- ☐ Manage Default Accounts on Enterprise Assets and Software
- ☐ Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- ☐ Establish and Maintain an Inventory of Accounts
- ☐ Use Unique Passwords
- ☐ Disable Dormant Accounts
- ☐ Restrict Administrator Privileges to Dedicated Administrator Accounts
- ☐ Establish an Access Granting Process
- ☐ Establish an Access Revoking Process
- ☐ Require MFA for Externally Exposed Applications
- ☐ Require MFA for Remote Network Access
- ☐ Require MFA for Administrative Access
- ☐ Establish and Maintain a Vulnerability Management Process
- ☐ Establish and Maintain a Remediation Process
- ☐ Perform Automated Operating System Patch Management
- ☐ Perform Automated Application Patch Management
- ☐ Establish and Maintain an Audit Log Management Process
- ☐ Collect Audit Logs

- ☐ Ensure Adequate Audit Log Storage
- ☐ Ensure Use of Only Fully Supported Browsers and Email Clients
- ☐ Use DNS Filtering Services
- ☐ Deploy and Maintain Anti-Malware Software
- ☐ Configure Automatic Anti-Malware Signature Updates
- ☐ Disable Autorun and Autoplay for Removable Media
- ☐ Establish and Maintain a Data Recovery Process
- ☐ Perform Automated Backups
- ☐ Protect Recovery Data
- ☐ Establish and Maintain an Isolated Instance of Recovery Data
- ☐ Ensure Network Infrastructure is Up-to-Date
- ☐ Establish and Maintain a Security Awareness Program
- ☐ Train Workforce Members to Recognize Social Engineering Attacks
- ☐ Train Workforce Members on Authentication Best Practices
- ☐ Train Workforce on Data Handling Best Practices
- ☐ Train Workforce Members on Causes of Unintentional Data Exposure
- ☐ Train Workforce Members on Recognizing and Reporting Security Incidents
- ☐ Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- ☐ Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- ☐ Establish and Maintain an Inventory of Service Providers
- ☐ Designate Personnel to Manage Incident Handling
- ☐ Establish and Maintain Contact Information for Reporting Security Incidents

5. **Record Request & Information Disclosure Policies**
    a. Only authorized employees shall disclose, share, send, or provide customer personal information to third parties.
    b. In general, customer records containing personal information should not be mailed, emailed, texted, faxed, or otherwise transmitted electronically. Whenever possible, employees authorized to provide customer records containing personal information shall require the customer to pick up the records in-person after being required to present a valid government-issued photo identification. If the person cannot reasonably be expected to visit the dealership, the person's identity must be verified using both of the following methods:
        i. Requesting they fax a copy of a valid government-issued photo identification;
            1. In the event a customer prefers to email or text their license, employees have an obligation to inform the customer that [Dealership_Name] DOES NOT endorse, recommend or request sensitive information be sent via email. Furthermore, employees are prohibited from accepting such information in the form of a text,

whether on a company or personal phone. A customer who insists on sending information via email should be informed of the risks of sending information over an unencrypted network and that faxing or providing in-person are safer alternatives.

ii. Asking the person to do a video meeting where the customer holds up their government-issued ID next to their face.

iii. Requesting the person's full name and at least two other identifiers such as date of birth, address, phone number, last four digits of Social Security Number, email address, VIN, or name of the salesperson who assisted them.

c. [Dealership_Name] personnel handling record requests have an obligation to securely destroy and shred customer information obtained in the process of verifying a customer's identity (e.g. shredding a faxed government-issued photo ID).

d. In no event may documents containing sensitive customer information (e.g., financial information, Social Security Number, credit information, and identification cards) be mailed or electronically transmitted. Customers must retrieve such documents from the dealership in-person after presenting a valid government-issued photo identification.

e. To the extent possible and reasonable under the circumstances, sensitive information should be redacted from files prior to them being released to the customer.

f. Unless required by state or federal law, under no circumstance shall a DMV Registration Inquiry Report ("KSR" or similar report from a state motor vehicle department) or Consumer Credit Report be provided to a customer or other third party.

g. In regard to service records, a customer is only entitled to records related to the period for which he/she was the owner of the vehicle in question. Employees have an obligation to review service records prior to release in order to ensure the customer is only receiving information pertaining to his/her period of ownership.

h. In general, customer records containing personal information should not be provided to unaffiliated third parties (e.g., vendors, manufacturers, and financial institutions) unless doing so is (1) required by law, (2) required to process a transaction initiated or requested by the consumer or (3) pursuant to a valid subpoena.

i. Special rules under state and federal laws govern the disclosure of information related to victims or potential victims of identity theft. Employees should contact competent legal counsel regarding requests related to identity theft.

7. Service Provider Oversight

[Dealership_Name] will oversee each of its service providers and processor that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

1. Evaluating the service provider's or processor's ability to implement and maintain appropriate security measures, consistent with this ISP and all applicable laws and

[Dealership_Name]'s obligations. This may include having the service provider or processor complete a vendor risk assessment questionnaire.

2. Requiring the service provider or processor by contract to implement and maintain reasonable security measures, consistent with this ISP and all applicable laws and [Dealership_Name]'s obligations. This may include having the service provider or processor complete and sign an applicable Data Processor Agreement.

3. Monitoring and auditing the service provider's or processor's performance to verify compliance with this ISP and all applicable laws and [Dealership_Name]'s obligations.

8. IT Change Management Policy

Changes to [Dealership_Name]'s IT infrastructure introduces a heightened risk of cybersecurity incidents. Accordingly, this section governs the addition, removal, or modification of the elements of [Dealership_Name]'s IT infrastructure as follows:

1. **Adding and removing end-user devices**. The Program Coordinator or designated IT personnel must be involved in adding end-user devices. Adding end-user devices, such as desktops, laptops, phones, or tablets requires that the devices be securely configured in accordance with the technical and electronic safeguards outlined in this policy. This includes, but is not limited to, automatic session locking after a defined period of inactivity, strong password requirements, and device lockouts after a specified number of failed authentication attempts. If possible, portable devices should be set up to support remote wiping of all company data upon suspected theft, loss, or employee termination.

2. **Adding third-party software & applications**. Prior to adding any third-party software or applications (whether hosted on premises or cloud-based), the vendor must be assessed for the adequacy of their technical and physical information safeguards. This includes, at a minimum, completing an electronic vendor risk assessment questionnaire for the service provider.

3. **Additions or modifications to web browsers**. Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. Accordingly, before allowing any browser to execute on the network, the following must be ensured:
    - Browser plugins are limited to trusted sources or otherwise disabled. Many plugins come from untrusted sources, and some are even written to be malicious. Therefore,

it is best to prevent users from intentionally or unintentionally installing untrusted plugins that might contain malware or critical security vulnerabilities.
    - Automatic updates and patches for the browser and plugins have been properly configured.
    - Content filters for phishing and malware sites have been enabled.
    - Pop-up blockers have been enabled. Pop-ups can host embedded malware directly or lure users into clicking links using social engineering tricks.

4. **Major additions or modifications to servers, operating systems, or network elements**. Any major modification, addition, or removal of servers, operating systems, or network elements (e.g., routers, switches, and firewalls) must be accompanied by the following:
    - A full internal penetration test.
    - A full internal and external vulnerability assessment.
    - Consider conducting a technical risk assessment that is designed to assess the safeguards outlined in this Program, as appropriate based on the changes made.

9. Data Retention Plan

The information of [Dealership_Name] is important to how it conducts business, protects customer data, and manages employees. If the dealership already has a records retention policy, this document can (and should) reference that policy. Or, the other policy can be discarded if it is out-of-date. Federal and state law require [Dealership_Name] to retain certain customer records, usually for a specific amount of time. [Dealership_Name] must retain certain records because they contain information that (1) serves as [Dealership_Name]'s corporate memory, (2) have enduring business value, or (3) must be kept to satisfy legal, accounting, or regulatory requirements. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for [Dealership_Name] and/or its employees:

- Fines and penalties.
- Loss of rights.
- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

This policy is part of a company-wide system for the review, retention, and destruction of records that [Dealership_Name] creates or receives in connection with the business it conducts. Any type of information created, received, or transmitted in the transaction of [Dealership_Name]'s business, regardless of physical format (collectively “record” or “records” hereinafter) are covered by this policy. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs and online applications.

- Contracts.
- Deal files.
- Electronic files.
- Emails.
- Handwritten notes.
- Hard drives.
- Invoices.
- Letters and other correspondence.
- Memory in cell phones and mobile devices.
- Online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, and other social media platforms and websites.
- Repair files.
- Voicemails.

Therefore, any paper records and electronic files that are part of any of the categories listed in the Records Retention Schedule contained in this policy must be retained for the amount of time indicated in the Records Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Program Coordinator or legal counsel.

[Dealership_Name] prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of [Dealership_Name] and retained primarily for reference purposes.
- Spam and junk mail.

How and When to Destroy Records

[Dealership_Name]'s Program Coordinator is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. Regarding customer information, if no record retention period is specified, the secure disposal of customer information in any format must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes. The destruction of confidential, financial, customer and personnel-related records must be conducted by shredding. The destruction of electronic records must be coordinated with the Program Coordinator. The destruction of records must stop immediately upon notification from legal counsel that a litigation hold is to begin because [Dealership_Name] may be involved in a

lawsuit or an official investigation (see below). Destruction may begin again once legal counsel lifts the relevant litigation hold.

Litigation Holds and Other Special Situations

[Dealership_Name] requires all employees to comply fully with its published records retention schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or legal counsel informs you, that [Dealership_Name] records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until legal counsel determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold and replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact legal counsel. In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of [Dealership_Name] with another organization or the replacement of [Dealership_Name]'s information technology systems.

Periodic Review & Other Responsibilities

The Program Coordinator shall periodically review this policy and its procedures with legal counsel and/or [Dealership_Name]'s certified public accountant to ensure [Dealership_Name] is minimizing the unnecessary retention of data to the extent possible and is in full compliance with relevant new or amended regulations. The Program Coordinator (or a more qualified individual as determined by the Program Coordinator) is responsible for identifying the documents that [Dealership_Name] must or should retain, and determining, in collaboration with legal counsel, the proper period of retention. The Program Coordinator also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Program Coordinator is responsible for the destruction of records whose retention period has expired.

Record Retention Schedule

Occasionally, [Dealership_Name] establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no business reason for doing so and consult with the Program Coordinator or legal counsel if unsure.

[Insert Data Retention Schedule. Dealer's may choose to use the NJ CAR Record Retention Schedule, available online at njcar.org]

10. Enforcement

Violations of this ISP may result in disciplinary action, up to and including termination, in accordance with [Dealership_Name]'s human resources policies.

11. Program Review

[Dealership_Name] will review this ISP and the security measures defined herein at least annually, or whenever there is a material change in [Dealership_Name]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information. [Dealership_Name] shall retain documentation regarding any such program review, including risk assessment, mitigation steps, disciplinary actions, and remediative actions.

12. Incident Response Plan

Purpose & Goals

The purpose of this Incident Response Plan (IRP) is to outline the responsibilities of the Program Coordinator for responding to "information security incidents". "Information security incident" means an actual or reasonably suspected event that has one or more of the following consequences:

1. loss or theft of personal information;
2. unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of personal information that may reasonably compromise the privacy or confidentiality, integrity, or availability of personal information; or
3. unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of [Dealership_Name]'s IT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of personal information or [Dealership_Name]'s operating environment or services.

Specifically, [Dealership_Name]'s goals for this IRP include to:

- Define [Dealership_Name]'s cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assist [Dealership_Name] and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.
- Mitigate or minimize the effects of any information security incident on [Dealership_Name], its customers and employees.
- Help [Dealership_Name] consistently document the actions it takes in response to information security incidents.
- Reduce overall risk exposure for [Dealership_Name].
- Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in [Dealership_Name]'s information security program and incident response process.

Accountability

[Dealership_Name] has designated the Program Coordinator to implement and maintain this IRP. Additionally, the Program Coordinator is responsible for coordinating each of the internal processes for responding to information security incidents, as defined in more detail below.

Internal Processes for Responding to Information Security Incidents

[Dealership_Name] may, from time to time, approve and make available more specific procedures for certain types of information security incidents. Those additional procedures and checklists are extensions to this IRP. The Program Coordinator may assign the duties of responding to an information security incident to other employees, departments (e.g., Human Resources, Legal, Information Technology) and external individuals, including vendors, service providers, or other resources, to participate in this IRP.

Upon identification of an information security incident, the Program Coordinator shall move quickly to perform the following steps, as applicable:

1. **Secure the dealership's operations**. The Program Coordinator, in conjunction with qualified IT personnel, shall be responsible for performing each of the following:
    1. Secure systems and fix vulnerabilities that may have caused the breach.
    2. Secure physical areas potentially related to the breach. Lock them and change access codes, if needed.
    3. Ask a forensics expert or law enforcement when it is reasonable to resume regular operations, if applicable.
    4. Mobilize a breach response team to prevent additional data loss. The exact steps to take depend on the nature of the breach, but should normally include [Dealership_Name] 's forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and executive management.
    5. Consider hiring independent forensic investigators to help determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.
    6. Consult with legal counsel and consider hiring outside legal counsel with privacy and data security expertise to advise on federal and state laws that may be implicated by a breach.
    7. Stop additional data loss by taking all affected equipment offline immediately, but don't turn any machines off until forensic experts arrive.
    8. Closely monitor all entry and exit points, especially those involved in the breach.
    9. If possible, put clean machines online in place of affected ones.
    10. Update credentials and passwords of authorized users. If a hacker steals credentials, systems will remain vulnerable until those credentials are changed, even if the hacker's tools have been removed.
    11. Remove improperly posted information from the web. If the incident involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or "cache," information for a period of

time. Contact the search engines to ensure that they don't archive personal information posted in error.
12. Search online for exposed data to make sure that no other websites have saved a copy. If you find any, contact those sites and ask them to remove it.
13. Interview employees who discovered the breach. Also, talk with anyone else who may know about it.
14. Do not destroy evidence. Don't destroy any forensic evidence during your investigation and remediation.

2. **Remediate weaknesses and fix vulnerabilities**. The Program Coordinator, in conjunction with qualified IT personnel, shall be responsible for performing each of the following:
    1. If service providers, contractors, processors, or other third parties were involved in the information security incident, examine what personal information they can access and decide if their access privileges need to change. Also, ensure they are taking the necessary steps to prevent another breach from occurring. If your service providers say they have remedied vulnerabilities, verify that they really fixed things.
    2. Work with forensics experts to analyze whether any network segmentation plan was effective in containing the breach and make changes as necessary.
    3. Find out if measures such as encryption were enabled when the breach happened.
    4. Analyze backup or preserved data.
    5. Review logs to determine who had access to the data at the time of the breach and analyze who currently has access. Then determine whether that access is needed and restrict access if it is not.
    6. Once all identified weaknesses have been remediated, perform the following:
        1. A full internal penetration test.
        2. A full internal and external vulnerability assessment.
        3. Consider conducting a technical risk assessment that is designed to assess the safeguards outlined in this Program, as appropriate based on the information security incident.

3. **Develop a comprehensive communications plan**. The Program Coordinator, in conjunction with competent legal counsel and executive management, shall perform each of the following:
    1. Verify the types of information compromised, the number of people affected, and whether contact information is available for those people.
    2. Develop a comprehensive communications plan that reaches all affected audiences — employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach and don't withhold key details that might help consumers protect themselves and their information. Ensure that there is no information disclosed in the communications that might put consumers at further risk.

3. Anticipate questions that people will ask. Consider putting together a list of frequently asked questions (FAQs) that can be displayed on your website or provided to customer-facing employees who might be asked about the incident. Make sure to use plain-language answers since good communication up front can limit customers' concerns and frustration, saving [Dealership_Name] time and resources later.

4. **Notify appropriate parties**. The Program Coordinator, in conjunction with competent legal counsel and executive management, shall perform each of the following:
    1. Work with legal counsel to determine applicable breach notification laws. All states, including New Jersey, have enacted legislation requiring notification of security breaches involving personal information. Depending on the circumstances and types of information involved in the incident, there may be several laws or regulations that apply, or none at all.
    2. Work with legal counsel to discuss notifying your local police department if there is a potential risk for identity theft. The sooner law enforcement learns about the incident, the more effective they can be. If local police aren't familiar with investigating information compromises, contact the local office of the Federal Bureau of Investigation or the U.S. Secret Service. For incidents involving mail theft, consider contacting the U.S. Postal Inspection Service.
    3. Work with legal counsel to discuss notifying affected businesses. For example, if credit card or bank account numbers have been stolen, but [Dealership_Name] does not maintain the accounts, notify the institution so that it can monitor the accounts for fraudulent activity. If the information compromised is collected or stored on behalf of other businesses, notify them of the incident.
    4. If Social Security Numbers have been stolen, work with legal counsel to discuss contacting the major credit bureaus and whether it is recommended that people request fraud alerts and credit freezes for their files.
    5. Work with legal counsel to discuss notifying individuals affected by the incident.
        1. Consult with law enforcement about the timing and content of the notification so it doesn't impede any active investigation.
        2. Designate a point person for releasing information.
        3. Consider offering at least a year of free credit monitoring or other support such as identity theft protection or identity restoration services, particularly if financial information or Social Security Numbers were exposed. When such information is exposed, thieves may use it to open new accounts. Depending on the circumstances, this may be required by law.
        4. Consider using the sample data breach notification letter below, which incorporates guidance from state and federal agencies, and consider creating a designated email or toll-free numbers to communicate with people whose information may have been compromised. If the contact information for all of the affected individuals is not available, consider building a press release or other news media notification. As part of any notification plan, consider enclosing with the letter a copy of "Identity Theft: A Recovery Plan," which is a

comprehensive guide from the FTC to help people address identity theft. The guide can be ordered in bulk for free at bulkorder.ftc.gov. The guide will be particularly helpful to people with limited or no internet access.

5. **Evaluate need for modifying incident response plan**. Following any information security incident, the Program Coordinator shall determine whether changes to this incident response plan are necessary and shall make such changes, as necessary, to improve the future handling of information security incidents. The Program Coordinator shall consider [Dealership_Name]'s effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The Program Coordinator shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

Sample Data Breach Notification Letter

[Insert Name of Company/Logo], Date: *[Insert Date]*

NOTICE OF DATA BREACH

Dear *[Insert Name]*:

We are contacting you about a data breach that has occurred at *[insert Company Name]*.

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].

What Information Was Involved?

This incident involved your *[describe the type of personal information that may have been exposed due to the breach]*.

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services)].

What You Can Do

[Insert the following language if the information compromised poses a high risk of identity theft or social security numbers were compromised].

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111
Experian: experian.com/help or 1-888-397-3742
TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

[Insert the following language if you choose to provide a copy of the FTC's identity theft guide].

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Other Important Information

[Insert other important information here]

For More Information

Call *[telephone number]* or go to *[Internet website]*. *[State how additional information or updates will be shared/or where they will be posted]*.

[Insert Closing]

[Your Name]

13. Effective Date

This ISP is effective as of [Date_Effective].

Please don't hesitate to contact us if you have any questions about this Compliance Manual.

info@complyauto.com
(385) 277-5882