Driven

NADA MANAGEMENT SERIES L43

A DEALER GUIDE TO THE

FTC Safeguards Rule

NADA NATIONAL AUTOMOBILE DEALERS ASSOCIATION

A DEALER GUIDE TO THE FTC SAFEGUARDS RULE

PREFACE

The purpose of this *Driven* Management Guide is to explain the Federal Trade Commission (FTC) revisions to the "Standards for Safeguarding Customer Information" issued under the Gramm-Leach-Bliley Act.[1] The FTC's Revised Safeguards Rule expands many requirements of the original 2003 rule and requires dealerships to revise their information security programs and implement new compliance measures by December 9, 2022. Additionally, this guide includes supplemental materials in the Appendices, including a sample information security program template at Appendix A to assist dealers in revising their information security program. That template is provided as a model only and should be adapted and modified by individual dealerships in light of the considerations explained in the guide and in consultation with legal counsel.

Dealers are required to revise their information security programs and ensure that they fully comply with the Revised Safeguards Rule by **December 9, 2022**.

Nothing in this guide (including the Appendices) is intended as legal advice. The requirements of the Safeguards Rule and the circumstances of every dealership are complex, and dealers should not simply adopt the sample information security program at Appendix A or any of its components, such as the incident response plan. In addition, this guide discusses only the FTC's Safeguards Rule; it does not discuss state or local law that may impose additional requirements, or requirements that may apply to you by contract. You should draft and implement all required policies and procedures appropriate to your dealership and ensure that they are fully reviewed by qualified legal counsel.

Note that some of the guidance presented in this publication is from an outside IT firm. This guidance is clearly marked as "IT GUIDANCE" and is not legal or compliance advice. Instead, it provides practical and important IT implementation guidance from a seasoned IT practitioner. As with all of the information in this guide, dealers should consult with their legal advisors to ensure compliance with the legal requirements of the Rule and other relevant legal requirements.

The presentation of this information is not intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

L43

Driven

A DEALER GUIDE TO THE

FTC Safeguards Rule

TABLE OF CONTENTS

A DEALER GUIDE TO THE

FTC Safeguards Rule

Section I: Introduction

By now, all dealers are familiar with the requirements of the Federal Trade Commission (FTC) "Standards for Safeguarding Customer Information" (Safeguards Rule), issued under Section 501(a) of the Gramm-Leach-Bliley Act (GLBA).[2] The Safeguards Rule was first issued in 2002, and took effect on May 23, 2003. It requires dealers to develop, implement and maintain a **comprehensive written information security program.**

On December 9, 2021, after several years of notice and comments, public hearings and debate, the FTC officially published revisions to its Safeguards Rule (Revised Safeguards Rule or Revised Rule), expanding many of the requirements applicable to dealerships.[3] The Revised Safeguards Rule requires dealerships to revise their information security programs and implement new compliance measures. This guide provides information and resources to aid dealerships in compliance. It does not provide legal advice; dealerships should consult with legal counsel as appropriate in ensuring compliance with the original and Revised Safeguards Rule.

The Revised Rule makes a few changes effective **January 10, 2022**. These new requirements are similar to the Rule's original requirements and likely will require only limited changes in practices for most dealerships. First, you are already required to conduct a **risk assessment** of existing threats to the security of your customer information and your information security safeguards, in order to establish sufficient safeguards in your information security program. The Revised Rule requires that you perform this risk assessment **on a periodic basis** going forward. We have provided more detail below on how to conduct a risk assessment and effectively implement it on a periodic basis (Section III, Step Two). Second, while you are already required to **regularly test or otherwise monitor** the key controls, systems, and procedures you use to safeguard customer information, the Revised Rule makes clear that this requirement includes **testing to detect actual and attempted attacks or intrusions** on your information systems. Section III, Step Four below provides more detail on regular testing or monitoring. The Revised Rule makes a few other near-term changes, including some changes to definitions.

The remaining new requirements—and most of the Revised Rule—are applicable on **December 9, 2022**. However, dealerships must take steps *in advance* to be in compliance on that date. The new requirements are discussed in greater detail in Sections II and III below. They will require **revision** of your information security program and **implementation** of new security measures. The new requirements include designating a "Qualified Individual" responsible for data security and implementing specific technical measures including encryption and multifactor authentication, regular penetration testing and vulnerability assessments for your information systems. This guide provides some tips on potential solutions on a streamlined or low-cost basis, but given the scope of these changes, dealerships need to identify and implement solutions throughout 2022 to ensure full compliance by the Revised Rule's December 9, 2022 deadline. Further, dealers need to plan for ongoing compliance after the Revised Rule becomes effective. This guide discusses strategies for compliance in Sections II and III below.

The Safeguards Rule applies broadly to all "financial institutions," including dealerships and other entities that provide or facilitate financial services. The intended purpose of the Rule is to protect consumer information from misuse or a data breach, and ultimately to protect your customers from identity theft or privacy violations. The revisions to the Rule have been issued in order to address a number of recent high-profile data breaches. Today, data breaches are in the news almost every day, and even smaller companies are targeted for "phishing, "ransomware," or other attacks that can result in exposure of personal information and significant harm to the targeted company and their customers. The Safeguards Rule provisions are meant to be applied to financial institutions of all

types and sizes,[4] and as a result, there is no one-size-fits-all approach.

Notably, dealerships should keep in mind that the GLBA Safeguards Rule is distinct from requirements under the GLBA Privacy Rule—which continues to separately apply.[5] The Privacy Rule deals with how you *share* information about consumers who obtain, or apply for, credit or lease products from you, and it includes specific notice requirements. The Safeguards Rule deals with how you *protect* information you receive from such consumers.[6] These obligations, while related, are independent of each other and subject to different standards, so you need to be careful that you take appropriate steps to comply with each.[7]

This guide explains the Revised Safeguards Rule and your obligations as automobile dealers to comply with it. Given the rise of ransomware threats and other cyberattacks during the COVID-19 pandemic, and the ease with which information can be transferred, accessed and altered, there is more reason than ever to be concerned about the threats of identity theft, document tampering and other misuse, compromise or misappropriation of customer data. The effects can be devastating to a consumer, and it can take years to undo the damage an identity thief can cause. From a dealership's perspective, there is also the potential liability arising out of customer information getting into the wrong hands. The Revised Safeguards Rule applies to all customer information in your possession, whether such information pertains to individuals with whom you have a customer relationship, or to the customers of other financial institutions that have provided that information to you. Accordingly, the protections it affords are likely relevant to **all of the customer personal information in your possession**.[8]

What kind of customer information is covered?

Technically, the definition of "customer information" includes only "nonpublic personal information" about a customer, which in turn includes only "personally identifiable financial information" about a customer. As the FTC has interpreted those terms, however, it can include nearly any information you collect from or about a customer. For example, "nonpublic personal information" includes lists or descriptions of consumers—including public information like names—if you derived them from non-public information you obtain from or about the consumers, e.g., customer lists. Separately, it also includes "personally identifiable financial information," which is any information "resulting from any transaction involving a financial product or service"—not just information that can be described as "financial." Moreover, it includes lists, descriptions, "or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."[9] In addition, in many of the enforcement actions brought by the FTC under the Rule (and throughout the commentary to the Revised Rule), the FTC has clearly applied the security requirements to all personal information, not just "nonpublic personal information." Accordingly, no one should think the Rule covers only sensitive information like Social Security Numbers or credit card numbers. Indeed, the Rule does not only apply to credit applications or information in finance or lease deals. On the contrary, out of an abundance of caution, you should treat the Rule as covering all customer-related information in your control or possession, whether in your dealer management system (DMS), customer relationship management (CRM), website or other system, in hard copy or electronic form, deal jackets or ROs, and in a dealer-owned computer or on your salesperson's cellphone.

To ensure compliance with the Revised Rule by the December 2022 deadline, start now to plan updates to your information security programs. The FTC (which enforces the Revised Safeguards Rule) has noted that Safeguards Rule requirements are not "one-size-fits-all," but nevertheless has made clear that certain steps and actions are required regardless of the risks involved. The FTC has provided a certain amount of flexibility in exactly how you meet each of the new requirements—but the big change in the amended rule is that *all* of the steps are now *required of all financial institutions*—including you.

IT GUIDANCE

From a technical point of view, satisfying a step can often be done via compensating control or existing security solutions. The guidelines should be approached by reviewing what currently exists before purchasing more technology.

Finally, please note that t**his guide does not address any state or local law requirements that may be applicable to your information safeguarding practices**. For example, safeguarding rules relating to insurance transactions between you and your customers may be promulgated by your state's insurance department. In addition, many individual states (and perhaps some localities) impose different and perhaps even more stringent safeguarding standards by statute or regulation. In some states, compliance with the Safeguards Rule may be required, or may mean you are treated differently under state privacy or security laws. It is critical that you work with your legal counsel to ensure that your information security program meets the standards not only of the Rule, but also of any applicable state or local laws.[10]

Section II: Overview

Applicability of the Revised Safeguards Rule

Are dealers covered by the Safeguards Rule?

The scope of the Safeguards Rule has not changed in relation to auto dealerships. Just as before, the Rule applies to all dealers who are "financial institutions" under Section 501(b) of the GLBA and are regulated by the FTC.[11] An entity is a financial institution if its business is either engaging in an activity that is financial in nature or incidental to financial activities. Incidental activities include such things as entering into finance or lease transactions with consumers.[12] This means that virtually all franchised new-car dealers (and all that offer or assist with financing or leasing) are subject to the Rule.

Does the Rule apply to medium- and heavy-duty truck dealers?

The Revised Safeguards Rule applies to information you obtain about "customers," and a "customer" must be a "consumer," which is defined to be an "individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."[13] Therefore, the Rule does not apply to information you collect about companies or individuals that obtain financial products or services for other purposes—such as business, commercial, or agricultural purposes.[14] This means that commercial transactions by medium- and heavy-duty truck dealers and wholesale light-duty transactions (to the extent the financing is between you and another business entity) may be outside the scope of the Rule. However, dealers should also keep in mind that, where they are engaged in even some transactions for personal, family, or household purposes, the Rule may be held to apply to those transactions. In addition, even though it may not technically apply to these transactions, dealers may want to ensure (for the reasons outlined above) that any personal information that you obtain in the course of such a transaction should be protected as highly as any other sensitive data.

What information is covered by the Revised Safeguards Rule?

The Revised Safeguards Rule requires you to adequately protect and safeguard "customer information."[15] Customer information is "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates."[16] "Customer" is defined, in turn, as "a consumer who has a customer relationship with you."[17] Therefore, you should subject all of your data about consumers to the protections of the Revised Safeguards Rule.

In general, customer information is information about a consumer with whom you have entered into a finance or lease transaction. This includes, for example, information contained in a consumer's credit report or credit application, account numbers, and bank balances. As explained above, however, it includes not only information about your customers **but also informa-**

tion you receive about the customers of other financial institutions (e.g., banks, finance companies, other dealerships).[18] Even lists of the names of your finance or lease customers would be covered by the Revised Safeguards Rule.[19] Note that for purposes of the Revised Safeguards Rule, customer information may include information you obtain from potential finance or lease customers—regardless of whether a lease or loan is extended—because those consumers may have a customer relationship with another financial institution.

As noted above, the definition of customer information should be treated broadly. Auto dealers are unique in that some of the information they gather could be deemed to be covered "customer information" depending on *how* it was gathered. For example, "personally identifiable financial information"—which is incorporated into the definition of "customer information"—includes any information: that a consumer provides to you to obtain a financial product or service from you; that resulted from any transaction involving a financial product or service between you and a consumer; or that you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.[20] Thus, even basic information like consumers' names can be treated as covered if provided in connection with a financial transaction.

The bottom line is that dealers should treat all customer information—whether on a credit application, in the CRM, on a repair order, or in a salesperson's phone—with the same high level of security and care as any other customer data. It is somewhat unclear what the FTC believes to be the scope of the Rule but given the Rule's broad definitions and the agency's enforcement actions and guidance it has provided, dealers should assume that the FTC believes that ALL customer data must be protected. Thus, it would be prudent to apply the Safeguards Rule protections to all of your customer data.

You should work with your legal counsel to determine the scope of your duties under the Rule and under any state or local data protection laws with which you must also comply.

When is the Revised Safeguards Rule effective?

As explained above, the majority of the new requirements detailed in the Revised Safeguards Rule take effect on **December 9, 2022**. However, a few new obligations—including planning for periodic data security risk assessments—are effective beginning on **January 10, 2022**.

Revised Safeguards Rule Requirements

Details about each requirement are provided below. In brief, the new requirements include:

1. **The designation of a "qualified" employee to oversee information security.**
2. **Preparation of a series of written documents, including:**
    a. **A written security risk assessment.**
    b. **A written "information security program," revised to include new requirements.**
    c. **A written "incident response plan."**
    d. **Written reports to the board of directors (or equivalent) about information security.**
3. **Implementation of specific IT technical requirements, including:**
    a. **Encryption.**
    b. **Multifactor authentication.**
    c. **Systems monitoring, penetration testing, and vulnerability assessments.**
4. **Implementation of specific procedural requirements, including the development and ongoing monitoring of:**
    a. **Access controls to customer information.**
    b. **Inventory of systems that handle customer information.**
    c. **Secure software development and utilization practices.**
    d. **Disposal procedures for customer information.**
    e. **Change management procedures.**
5. **Employee training requirements.**
6. **Periodic review of service providers' security practices.**

The Core Requirement: A Comprehensive Written Information Security Program

The Safeguards Rule requires you to develop, implement and maintain a comprehensive written information security program, and the Revised Safeguards Rule expands the specific requirements that must be included.

THIS MEANS THAT YOU NEED TO HAVE A REVISED PHYSICAL, WRITTEN DOCUMENT BY DECEMBER 9, 2022 that outlines your dealership's policies and procedures relating to the physical, administrative, and technical safeguards you have in place to protect customer information. Your information security program must be comprehensive. That is, it must fully address the information security risks in all areas of your operations. It may be contained in one or more documents. For example, the part of your program applicable to employee training and management could be contained in a section of your dealership's policies and procedures relating to employees.

The FTC does not provide a template or require specific language in your written information security program. Instead, the Revised Rule requires that the information security program meet certain objectives and address certain specific elements.

Program objectives

The Revised Safeguards Rule requires that your information security program meet these three objectives:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security and/or integrity of customer information.
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

Eight required elements

The Revised Safeguards Rule requires that the following eight elements are included in your information security program. Each element is discussed in detail in Section III.

1. You must designate a "Qualified Individual" responsible for overseeing, implementing, and enforcing your information security program. This person may be an employee or a third party overseen by a senior member of your personnel.

IT GUIDANCE

Although the Rule permits outsourcing security, responsibility for the program cannot be outsourced. From a practical standpoint, in a smaller dealership the Qualified Individual may be the office manager or other staff member. The Rule does not require dealership staff to implement the program at a technical level; rather, your Qualified Individual *must* provide oversight to ensure that implementation is done, in many cases by an outsourced provider.

2. You must periodically conduct risk assessments to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise, and assess the sufficiency of any safeguards in place to control these risks. You must keep a written record of your risk assessments. You must base your information security program on these risk assessments. The assessments should include:
    - Criteria for the evaluation and categorization of identified security risks or threats you face.
    - Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face.
    - Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
3. You must design and implement customer information safeguards to control the risks you identify through the risk assessment. Such safeguards must include:
    - Access controls.
    - Taking system inventory.
    - Encryption.
    - Secure development practices.
    - Multifactor authentication.
    - Disposal procedures.
    - Change management procedures.
    - Monitoring and logging of authorized user activity.

IT GUIDANCE

The risks enumerated here are also consistent with many requirements under the Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST) and Center for Internet Security Top 20 Critical Security Controls (CIS20). Implementation of the required policies, procedures and controls under the Rule can also be used to satisfy other potentially applicable compliance requirements.

4. You must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, your information systems. Testing must include either continuous monitoring or annual penetration testing and vulnerability assessments conducted at least every six months.

5. You must implement policies and procedures to ensure that your personnel are able to enact your information security program by:

    - Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment.

IT GUIDANCE

If you are unsure where to start, your IT provider should be able to provide you with simple, inexpensive security awareness training based on email and web applications.

    - Utilizing qualified information security personnel, employed by you or an affiliate or service provider, sufficient to manage your information security risks and to perform or oversee the information security program.
    - Providing information security personnel with security updates and training sufficient to address relevant security risks.
    - Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

6. You must oversee your service providers that have access to customer information by:

    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for your customer information.
    - Requiring your service providers by contract to implement and maintain such safeguards.
    - Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

IT GUIDANCE

Ensure that your provider can produce regular proof of the services being provided. For example, the provider should be able to produce and give you a meaningful report that flags any issues, as opposed to a log of tickets or calls.

7. You must establish a written incident response plan designed to assist in quickly responding to and recovering from a security incident involving the exposure of customer information. Your written incident response plan should include the following elements:

    - The goals of the plan.
    - The internal processes for responding to a security event.
    - The definition of clear roles, responsibilities, and levels of decision-making authority.
    - External and internal communications and information sharing.
    - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.
    - Documentation and reporting regarding security events and related incident response activities.
    - The evaluation and revision as necessary of the incident response plan following a security event.

IT GUIDANCE

It is critical that your incident response plan is a business-level plan rather than an IT department plan. Technical staff should know which dealership executive(s) to contact in case of an incident and ensure that the proper executives include those responsible for legal and insurance resources.

8. Your Qualified Individual must report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be presented in a timely manner to a senior officer responsible for your information security program. The report shall include:

    - The overall status of the information security program and your compliance with the Rule.
    - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses to them, and recommendations for changes in the information security program.

Individual plans will vary by the complexity of dealership operations

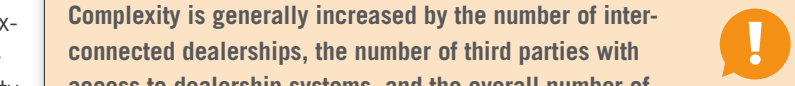
As noted above, the FTC's Revised Safeguards Rule contains a number of very specific elements that must be implemented as part of an information security program. At the same time, the FTC has tried to fashion the Revised Safeguards Rule's requirements to be flexible enough to cover large and small financial institutions alike.[21] Under the Rule, your information security safeguards must be appropriate for:

- The size and complexity of your dealership and its operations.
- The nature and scope of your dealership's activities involving customer information.
- The sensitivity of the customer information that you handle in any way.

Therefore, while all dealerships are required to implement plans with certain specific elements, individual dealerships may implement different programs based on the scope of their own operations and their assessment of security risks. For example, larger dealerships may have larger and more complex IT systems and data-sharing relationships, which could create more opportunities for information misappropriation and therefore require more complex safeguards policies. On the other hand, smaller dealerships may have more streamlined systems for dealing with customer information and may adopt less complex policies while ensuring that they meet all of the required elements.

IT GUIDANCE

Complexity is generally increased by the number of interconnected dealerships, the number of third parties with access to dealership systems, and the overall number of applications and systems a dealership uses.



What does this all mean?

The requirements we've outlined can provide some guidelines for drafting your information security program, but there is no FTC-prescribed language or form that you must use. Thus drafting the program can be complicated, but note the following:

First, by properly drafting and implementing your information security program, you are by default meeting many of the other requirements of the Revised Rule, as the information security program must address many of these issues. We have provided a step-by-step guide to this process below.

In addition, we have provided a sample information security program at Appendix A. That sample is just an *example* of an information security program. *You should not simply adopt the sample as it appears in this guide*. Look to the sample for guidance, but it is critical that you adjust and modify your dealership's information security program to your specific facts, operations, and systems. Work with your IT experts, vendors, and legal counsel to ensure this critical step is completed properly.

Penalties for not complying with the Revised Safeguards Rule

The penalties for not complying with the Revised Safeguards Rule can be extensive—and expensive. The FTC can initiate an enforcement action against automobile dealers under the authority granted to them in the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq*. Penalties may include long-term consent decrees with your companies and sometimes your executives, extensive injunctive relief, and potential monetary fines for violations of the consent decree. While the FTC cannot seek monetary penalties for first-time violations of the Safeguards Rule, it often seeks to identify violations for which it otherwise can seek money. Further, the FTC can seek up to **$46,517** per consent order violation, and the FTC can take an expansive view of what a "violation" is, depending on the circumstances—particularly if there are issues involving multiple customer records.

The Revised Safeguards Rule does not permit an individual (or a class of individuals) to bring a lawsuit against you for violating the rule. However, you could be subject to claims (including class action claims) under the "unfair and deceptive acts and practices" (UDAP) laws of the various states for failure to comply with the Safeguards Rule.[22] These laws typically permit actual and punitive damages, as well as attorneys' fees and costs. In addition, a state Attorney General could bring an action against you under the same types of state laws. Further, any data breach is generally governed by state law, and you should consult with your attorney about possible liability and reporting requirements under state law.

Section III: A Step-by-Step Guide to Developing, Implementing, and Maintaining Your Information Security Program

This Section contains a step-by-step guide for developing an information security program. There is no requirement in the Revised Rule that you take each of the steps listed in the order they are presented. For example, you may take a system inventory (Step Three) as part of your risk assessment (Step Two). These steps are listed as follows solely for clarity and ease of presentation. But you *must* take each step by the compliance deadline of December 9, 2022, in whatever order you deem best for your dealership. Your revised written information security program, which should document each of the steps, should also be prepared by December 9, 2022.

STEP ONE: Designate a "Qualified Individual" to Oversee, Implement, and Enforce Your Information Security Program

Under the Revised Safeguards Rule, you must appoint a "Qualified Individual" (a position similar to the information security "Program Coordinator" already required)[23] who will be responsible for developing, overseeing, and enforcing your information security program. This individual will also be required to report annually to your company's board of directors or other top leadership about the status of the dealership's information security program.

What are the Qualified Individual's Job Responsibilities?

Your Qualified Individual is responsible for overseeing, implementing, and enforcing all aspects of your infor-

mation security program. This includes, as described in greater detail below:

- Overseeing and implementing periodic risk assessments.
- Coordinating regular employee information security training.
- Implementing mandatory safeguards and testing and auditing those safeguards.
- Supervising service providers that handle customer information.
- Designing and overseeing the drafting of a written incident response plan.

Accordingly, while "coordinating" information security programs is the responsibility of your Program Coordinator(s) under the prior iteration of the rule, the Revised Safeguards Rule now requires the appointment of a *single Qualified Individual* in charge of executing and maintaining your information security program.

Moreover, as explained in greater detail below, and similar to the Program Coordinator role, your Qualified Individual should report directly to a senior member of your dealership, and your board of directors if your business has a board. That report must be in writing (addressed in more detail in Step Eight below). Additionally, your Qualified Individual has the authority to design specific information security safeguards for your business, as described below in Step Three. In many respects, therefore, your Qualified Individual will have the same duties as your Program Coordinator(s).

What Does It Mean to be a "Qualified" Individual?

Although your Qualified Individual must have some level of information security training and knowledge, that person does not necessarily need to be a data security expert or Chief Information Security Officer.[24] The Revised Safeguards Rule does not require your Qualified Individual to hold a particular level of education, experience, or certification.

Rather, you may select the person who is appropriate for the needs of managing your information systems and the customer data you collect. The FTC has indicated that the necessary qualifications "will depend upon the size and complexity of a financial institution's information system and the volume and sensitivity of the customer information the financial institution possesses or processes."[25] If you run a small- to medium-sized dealership whose information systems do not possess or process as much customer information as a large dealership, your Qualified Individual will need less training and expertise than a Qualified Individual responsible for a dealership with large, complex information systems.

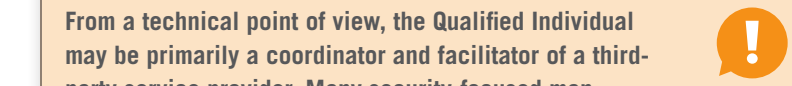
In many instances, the Program Coordinator you already have may be appropriate for the Qualified Individual role based on his or her role in testing and evaluating current information safeguards. However, if you appoint the same individual, you should note that the Qualified Individual is responsible for implementing many more detailed requirements under the Revised Rule, and the individual may need to have a higher level of training and technical familiarity to effectively implement your information security program.

Compliance Tip

Before choosing a Qualified Individual, you should review the detailed technical requirements in Step Three below and the requirements for a written report to the board in Step Eight, and ensure your Qualified Individual has sufficient expertise to perform those functions. Even if the Revised Rule does not require formal training, the Qualified Individual will need to effectively document compliance in the annual report to the board.

IT GUIDANCE

From a technical point of view, the Qualified Individual may be primarily a coordinator and facilitator of a third-party service provider. Many security-focused managed services providers can address the majority of the requirements for board interaction as well as program development and implementation of solutions.



It is also relevant to note here that the FTC's stated purpose for requiring that *one person* be appointed in this role is so that *one person* will be accountable for issues that may arise. This does not mean that the Qualified Individual may not delegate responsibilities, nor does it mean that the Qualified Individual will be specially liable in the event of an issue. It does clearly mean however, that the Qualified Individual must be prepared to address and answer any security event or other issues that may arise under the information security program.

Additionally, under the Revised Safeguards Rule, an employee of affiliates or a service provider can serve as the Qualified Individual, which is a change from the previous Rule. That option is discussed in more detail below.

What Must I Do if I Hire a Third-Party Vendor to Serve as a Qualified Individual?

As noted above, the Revised Rule permits you—if you choose—to appoint a third-party vendor employee to fulfill the role of a "Qualified Individual." The FTC has, for example, pointed favorably to using virtual services provided by third parties that can provide security support for many companies, effectively splitting the cost among companies, and that may also provide additional services such as built-in encryption and multi-factor authentication.[26] You may also use third parties that provide services in-person. Use of third-party vendors may be attractive for small- to medium-sized dealerships that wish to utilize lower-cost options.

If your dealership designates a vendor as your Qualified Individual, you retain ultimate responsibility for the actions of the third-party Qualified Individual and you must follow certain steps:

- You must designate senior personnel to oversee the third-party Qualified Individual.
- The third-party Qualified Individual must implement an information security program that is compliant with the Revised Rule to protect your customer information.
- While the senior personnel that you select to oversee a third-party Qualified Individual need not be an expert in information security, the individual must supervise and monitor the third party so that the dealership is aware of its data security needs and the safeguards being used to protect its information systems.

Compliance Tip

As NADA noted in comments to the FTC, the requirement to appoint a "senior employee" to oversee and monitor a third party in this role tends to undermine any efficiencies potentially gained by such an appointment. You must make your own decision about whether to outsource this role but note that it is not enough to simply outsource the role—you must oversee the third party to make sure you meet your continuing obligations under the Revised Rule.

IT GUIDANCE

If you wish to identify a capable third party to serve as your Qualified Individual, ensure that the third party provides a co-managed program and furnishes reports/proofs of self-validating the security solutions. Generally, this is not supplied by the same vendor providing PC and end-user support

How Many Qualified Individuals May I Designate?

You may designate only one person in your business as the Qualified Individual responsible for overseeing and enforcing your information security program. However, you may still assign information security duties and responsibilities to other staff, and the Qualified Individual may have other workplace responsibilities aside from the information security program. If your Qualified Individual departs your dealership, you should immediately reassign those responsibilities to another individual with sufficient qualifications.

Are Any Formal Reports Required from the Qualified Individual?

The Revised Safeguards Rule requires that your Qualified Individual make *written* reports on at least an annual basis to your board of directors. If your company does not have a board of directors, then your Qualified Individual must make this report to a senior company official responsible for overseeing your information security program. These reports are discussed in greater detail in Step Eight, below.

When Must I Designate My Qualified Individual?

Under the FTC's Revised Safeguards Rule, dealerships are required to designate their Qualified Individuals by December 9, 2022. As a practical matter, in order to fully comply by the deadline, you need to designate this individual much sooner. Indeed, it is advisable to designate your "Qualified Individual" as soon as feasible so that individual can address the myriad other requirements of the Revised Rule.

STEP TWO: Conduct Risk Assessments on Information Security and Existing Safeguards

What is a Risk Assessment?

In the context of the Safeguards Rule, a risk assessment (1) evaluates internal and external security risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information; and (2) assesses the sufficiency of any safeguards in place to control these risks. The 2003 Rule already requires this kind of assessment, but the Revised Rule specifies that beginning on January 10, 2022, you must base your information security program on this assessment. You must also plan to conduct such risk assessments periodically, to reassess such risks and safeguards. Additionally, as of December 9, 2022, this risk assessment must be in writing, and it must contain certain elements discussed below.[27]

What's New?

You have always been required to conduct a risk assessment as part of your Safeguards Rule compliance. It makes sense really: How can you effectively secure your customer data if you don't try to analyze what risks your dealership faces? So, what is new? Basically:

1. The risk assessment has to be written. Previously, the only written document you needed to have was a written information security program. Now, an additional written document is required for compliance.
2. You have to conduct such assessments "periodically." While it is unclear exactly what this means, one thing is clear: This is not a "set it and forget it" requirement. You have to update your assessment and keep up with key changes to ensure you are assessing the real, current risks involving customer information.

How Often Must I Conduct Risk Assessments?

Beginning on January 10, 2022, you must conduct risk assessments "periodically." The Revised Rule does not clarify what that means nor does it include any precise requirement of how often assessments should be conducted. However, it would seem appropriate to undertake a risk assessment at least annually, or more often as circumstances warrant.

Steps to consider include:

- Establishing a predetermined schedule to

ensure that the risk assessments occur and are documented in a timely manner.

- Ensuring that you conduct and document risk assessments when there any changes in your dealership's information systems, and to account for any security threats that those systems may encounter as the threats evolve. This should be consistent with your change management policy, discussed in Step Three, G below.
- Evaluating if an additional risk assessment should be conducted, in case of a security incident, to reexamine risks and the adequacy of your safeguards.
- Establishing a process to adjust your information security program based on your periodic risk assessments. If your risk assessment uncovers a new or heightened risk (or a lower risk), make sure that your written program addresses that risk.

IT GUIDANCE

A risk assessment should not be confused with a vulnerability scan. Scans are generally a quarterly process while risk assessments are once per year.

What Specific Factors Must My Risk Assessments Cover?

Beginning on December 9, 2022, risk assessments must be detailed in a written document and address each of the following:

- Criteria for the evaluation and categorization of identified security risks or threats that your information systems face.
    - This means that you should write out the categories of risks that you considered and identified. For example, and the following is not an exhaustive list: Have you identified risks from remote access and processing of customer information by employees? Are there risks from how you share information with vendors and other third parties? Are there areas in your IT network containing information that is more likely to be targeted by bad actors (e.g., containing sensitive financial information or Social Security numbers)?
    - Remember that risks include data security risks (like phishing, ransomware, or other cyber risks), but also risks to physical data. Evaluate, for example, whether drawers and offices (F&I) should be locked.
- Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face.
    - This means that you should write out the way in which you evaluated the adequacy of existing controls to address these risks. For example, and again, this is not an exhaustive list: Are there access controls to customer information currently in place, and how are they enforced? What kind of ongoing service provider oversight do you perform?
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
    - This means that you should document what actions will be taken to address risks as part of your information security program.

Compliance Tip

As part of the mandatory safeguards you must implement, you must conduct a system inventory of your data, personnel, devices, systems, and facilities used for business purposes, in order to understand where customer information is stored and how it is accessed. You may want to conduct the system inventory in connection with the risk assessment, for efficiency and to better inform the risk assessment.

IT GUIDANCE

When looking into where customer information is stored, the simplest and most accurate way to gather this data is by discussion with relevant personnel and vendors, backed by a programmatic scan of the environment.

STEP THREE: Implement Mandatory Safeguards to Control Risks

Once you have identified the risks, you must implement the appropriate safeguards to address those risks. While your dealership is already required to design and implement safeguards to control the risks identified in your risk assessments, the Revised Safeguards Rule adds more detailed requirements for what safeguards should be incorporated. As noted above, the Revised Rule contains a number of new safeguards that must be implemented as part of your information security program—regardless of your risk assessment.[28] These requirements include:

A. Access controls.
B. System inventory.
C. Encryption.
D. Secure development practices.
E. Multifactor authentication (MFA).
F. Disposal procedures.
G. Change management procedures.
H. Monitoring and logging of authorized user activity.

Implementation and policies related to each of these requirements should be documented in your written information security program. You are required to implement the specific safeguards listed above by December 9, 2022. Below we provide more detail about the requirements and options that you may have to implement them.

A. Access Controls. You are required to place access controls on all customer information, whether it is stored in information systems or physical locations, to permit access only to authorized users.[29] This requirement is intended to protect against the unauthorized acquisition of customer information. You should review your access controls periodically.

For electronic systems, you should require some form of authentication to permit access only to authorized users. Password protections on databases and files containing customer information also would be appropriate. Where customer information is kept in physical form, such as printed customer reports, physical access controls are required. These might include door locks or key card access systems to ensure unauthorized individuals cannot access the information.

IT GUIDANCE

Be careful with password protection, which can lead to data loss as there is no method for the company to recover the passwords. Password protection should apply to network access, PC access, and system/application access.

Moreover, even for authorized users, you should have a policy to permit personnel access to customer information only when needed to perform a specific function. Personnel should not be permitted to access customer information for purposes other than an authorized work function. Additionally, when a service provider or other vendor accesses your data or information systems, you must ensure that appropriate access controls are in place for them. You should not allow a service provider or other third party to access customer information unless it is necessary for the service provider or third party to do so for one of your business purposes.

B. System Inventory. You are required to identify and manage the data, personnel, devices, systems, and facilities that enable your dealership to achieve its business purposes, in accordance with their relative importance to business objectives and your risk strategy. This inventory should allow your Qualified Individual to have a full understanding of the relevant portion of your information systems and their relative importance. Specifically, this inventory must include all systems that are a part of the business so that your dealership can locate all customer information it controls, the systems that are connected to that information, and an explanation of how they are connected.

IT GUIDANCE

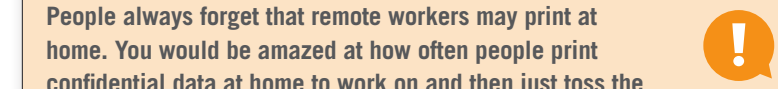
Inventories can be really hard for some companies, big and small. Some styles of risk assessment can be done without a full inventory because you are looking at the type of risk and type of attack. Full inventories tend to be more technical in nature. People can get so bogged down in inventorying they never get to the security part, which is counterproductive to safety. While an inventory is a critical part of the process, note that you can generally perform a risk assessment and begin access control just based on best practices and due diligence actions.

Your system inventory goes beyond your DMS and your CRM system. You need to identify and understand where customer information of any kind may exist at your dealership or in your systems or those of your service providers. You should consider other areas where customer information may be collected, stored, or shared, including but not limited to systems and devices such as:

- Your websites.
- Appointment scheduling software.
- Personal computers of employees working both remotely and onsite.
- Mobile phones of sales personnel, which may contain consumer names and phone numbers.
- Third parties that may store or process data on your behalf.
- And others

IT GUIDANCE

People always forget that remote workers may print at home. You would be amazed at how often people print confidential data at home to work on and then just toss the data into the recycling bin.



The systems inventory should be extensive, careful, and, thorough. Think outside the box. It could also include websites that are not your own (OEM sites for example), Wi-Fi networks, and even the vehicles themselves.

Ask yourself whether any of your customer information exists or *could* exist in those systems. If so, then you must understand what is there, who has access, and enough about the IT infrastructure to determine issues like:

- Who has access to that data?
- Could bad actors access that data, and if so, how?
- With whom is that data shared, and are the controls on those third parties adequate?
- Could the data be lost or abused—by employees or non-employees?

Think broadly about your information systems and understand how your data is stored, where, and with whom. It's not enough to know that your data is housed at a third party; you must also understand who that third party shares customer data with and how it is safeguarded if shared.[30]

IT GUIDANCE

You may want to differentiate between data housed at a third party and data processed by a third party. In the first instance you generally are assuming more direct responsibility for security, regardless of what services that third party performs. In the second, where you use a third-party platform or software-as-a-service (such as a cloud CRM), data security is an integral part of the contract. As long as you are following required safeguards for user accounts and access, the third party should be the party primarily responsible for addressing the remaining security pieces. Work on this issue with your legal and IT professionals.

What If I Cannot Obtain This Information from a Vendor or Other Third Party?

This is a complicated, yet critical step, and it will require internal effort, along with complete transparency and cooperation from your IT vendors.

For many years, many dealers have been asking for just this information from their vendors and have met with difficulty in many circumstances. For more on service provider safeguards compliance, see the discussion of service providers below in Step Six, but for purposes of the system inventory, you should understand that this is a basic building block of your information security program. If you don't know everywhere that your data is, you cannot adequately protect it.

There may be instances where dealers continue to face resistance from vendors—either because of an unwillingness or inability by the vendor to assist. It is clear however, that you must have transparent, prompt, and complete answers from all your vendors, and have them in short order, if you are to be able to meet your obligations under the Revised Rule.

As the FTC has noted, "[s]ome high profile breaches have been caused by service providers' security failures, and the Commission views the regular assessment of the security risks of service providers as an important part of maintaining the strength of a financial institution's safeguards," and a "financial institution must be sure a service provider is protecting the information of its customers."[31]

If you cannot obtain this information, following the FTC's guidance, you should no longer do business with those vendors, and you should immediately demand return/deletion of all data.[32]

This is no small task, nor may it be a small issue if unresolved, but that does not change the fact that as the regulated entity you are responsible for this issue, and you must be firm in insisting on compliance from all vendors with whom you do business.

What about my OEM?

It is important to note that there is no exception or special treatment under the Revised Rule for your OEM. That means that if you share customer information with your OEM—either directly via a data-sharing agreement with the OEM as a service provider, or indirectly, via a third-party service provider—you must ensure that the same service provider provisions and protections are in place with respect to the relevant contract and to the OEM and any third party. We understand that historically it has been difficult at times to get some OEMs to agree to required contract terms, limitations, audit rights, or other basic data protections, but that does not mean it is not required. We are hopeful that the OEMs will understand that these new requirements and restrictions are required under the Revised Rule, and will agree to the contract amendments, practice and procedure changes, and audits required under the Revised Rule. NADA will continue to work with OEMs to explain the need for these changes.

NADA is conducting outreach to vendors to educate them about the need for this information, and about the other expanded service provider obligations outlined herein.

C. Encryption. You are required to encrypt all customer information held or transmitted by you when **in transit over external networks** and when **at rest** (unless you use approved alternative controls, discussed below). For example, a database with customer loan information needs to be encrypted when the data is not actively being used. Customer data also needs to be encrypted when sent to third parties. However, data would not need to be encrypted when transmitted over internal networks, such as using internal email.

What is encryption? "Encryption" is defined in the Revised Rule as "the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material."[33] Essentially, as defined by the FTC, it is the process of encoding information so that it is unreadable unless someone has an "encryption key," or password, to decrypt the information.[34] It does not require any specific process or technology but "does require that whatever process is used be sufficiently robust to prevent the deciphering of the information in most circumstances."[35]

Again, this means that you must ensure that all customer data is encrypted in your internal dealership systems, as well as with your vendors to the extent any consumer data is shared with or stored by vendors. You should also encrypt all customer data when it leaves your internal networks, including when it is being shared with a third-party vendor.

There is a limited exception to this requirement if encryption of certain customer information is "infeasible," in which case you may instead secure such customer information using "effective alternative compensating controls" reviewed and approved by your Qualified Individual.[36] In short, you should rely on your Qualified Individual to identify areas in which encryption under the FTC's definition is not possible, and consider alternatives approved by your Qualified Individual.

IT GUIDANCE

In a nutshell, all customer data needs to be encrypted by a modern encryption program. Much of this is already done by default (but of course you must confirm and document), and there are a number of free and low-cost encryption solutions available to consider. Scrambling and obfuscation of data are not satisfactory. Also, while password protection of office documents adds encryption, use of them poses a strong risk of data loss.

What is an external network?

An external network refers to data traveling outside of the dealer's controlled systems—i.e., to a third party, a service provider via SaaS or cloud systems or email. As an example, a CRM used with a secured web browser is encrypted, and there may not be need to take any further action. In short, if you allow access to your systems from home, that access needs to be via a secure website or VPN. If you use an internet or cloud-based system, it also must be secured via secure website (HTTPS) or VPN. If you send information to vendors (such as a mailer company), it must be sent via encrypted files or encrypted email.

What is an internal network?

An internal network comprises the systems in a location that you control and are responsible for. All systems are behind a firewall that you control. An internal network can include multiple locations connected by a private network (MPLS or site-to-site VPN), but not work-from-home personnel.

What is "at rest"?

Data is "at rest" when no one is using it. For example, a spreadsheet or PDF that a customer saves to a PC or file-share would be considered "at rest." That said, "at rest" data can be encrypted in many ways that are more satisfactory to workflow and pose less risk than individual passwords per file. Compensating controls are critical in this area.

Finally, unless your Qualified Individual is experienced in highly technical security implementation, discuss alternatives to "infeasible" encryption with a subject matter expert to avoid undue cost, difficulty, and business interruption.

D. Secure Development Practices. You are required to implement secure development practices for applications that you develop to transmit, access, or store customer information. While some dealers may develop their own in-house applications, most

dealers use third-party software rather than developing their own. In these cases, you need to take steps to evaluate that the software you use is secure.

What exactly this requires is somewhat unclear. Based on FTC comments, it does not appear that you are required to review source code or undertake a sophisticated review of each of your vendors' infrastructure. The FTC notes that "a provider can supply the steps it took to ensure the software was secure, whether it uses encryption to transmit information, and the results of any testing it conducted."[37] Additionally, "[s]oftware that has been thoroughly tested by third parties may need little more than a review of the test results."[38]

Therefore, if you use a service provider to provide software, you should ask about all the security features of the software and whether the application uses encryption to store and transmit information (as noted above). You must ask for and review the results of any security testing it conducted. Further, you should more closely scrutinize service providers handling highly sensitive information (like financial information). Additional steps involved in overseeing service providers are discussed below.

IT GUIDANCE

Ask relevant service providers/vendors to confirm their use of "field-level encryption" for highly sensitive data.

You may elect to use a third party to evaluate software security, as noted above. However, if software has not been widely used and tested, you need to conduct a closer examination of information obtained from the software service provider.

IT GUIDANCE

While it may be advisable to seek confirmation of ISO compliance or other security certification to ensure your software is safe, that alone may not satisfy the requirements of the Rule. If a service provider is providing software-as-a-service (SaaS) or CRM-as-a-service, for example, their confirmation of secure coding practices would entail showing SOC2/3, PCI, and HIPAA compliance. It is important to note that you can't do a vulnerability scan on 99% of SaaS/Cloud providers. Work with your legal and IT experts to determine what certifications you should seek, and whether more (such as third-party IT audits) may be required.

The FTC also suggests that you can set up automated searches regarding vulnerabilities, patches, and updates to software that you use for customer information.[39] While not explicitly required by the Revised Rule, the FTC has begun to issue notices about specific vulnerabilities—for example, the "log4j" vulnerability—and indicated that it will take enforcement action against companies that fail to remediate "known" vulnerabilities. Therefore, you should take steps to automate or otherwise regularly check public sources that publish known software vulnerabilities.[40] Additional resources published by the U.S. Cybersecurity & Infrastructure Security Agency are included at Appendix B.

IT GUIDANCE

Make sure you know whether the software you use on internal systems is from service providers or SaaS providers. There are many third-party patch management systems, and most should include basic vulnerability scanning. For small dealerships that want to ensure security and compliance together, this is the best place to start. You may wish to consider outsourcing this scanning to ensure checks and balances between IT staff and the vulnerability scan. With the changes in technology it is important to use a scanning system managed from the internal environment running an authenticated scan.

There are also a number of free or low-cost vulnerability detection applications available.[41] You should consult with IT and legal experts to determine the appropriateness and adequacy of any such tool. Overall, there is no one-size-fits-all approach, and your review will depend on the nature of the software you use and how you store and transmit customer information.

E. Multifactor Authentication (MFA). You must implement either multifactor authentication or reasonably equivalent controls (with the approval of your Qualified Individual) whenever any individual —whether an employee, customer, or otherwise—accesses an information system containing customer information or another interface connected to a system containing customer information.

The Revised Safeguards Rule defines "multifactor authentication" as "authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as biometric characteristics."[42] One example of multifactor authentication is requiring an employee logging into a system to also enter a code sent to an app on their mobile device, in addition to entering a password.[43]

Compliance Tip

While this is certain to add steps and time when your employees log into the system, you should consider working with your IT vendor to limit such disruptions. Also, the FTC has noted that you can potentially limit cost and disruption from multifactor authentication and other technical requirements like encryption by segmenting your networks to isolate consumer information. As a result, authentication would only be required to access network locations with consumer data or a network connected to locations with consumer data. Again, work with your IT vendor to determine whether such segmentation of other restrictions can assist your implementation efforts.

IT GUIDANCE

With advances in basic Microsoft products and licensing as an example, MFA no longer needs to be burdensome to employees' workflow and processing. In fact, this requirement can be made simpler by adopting a proper authentication and single or integrated sign on architecture. This can also assist with compensating controls for other safeguard areas, simplify inventories, secure service providers, add security and make life easier for users (fewer passwords, training, and steps). Of all the safeguard areas, the enactment of a properly functioning MFA system will create the most safety and protection from the more common and frequent attacks/risks that occur. For actionable and proactive security, this is one of the primary areas that should be addressed.

IT GUIDANCE

Segmentation of the network to isolate consumer information, though very difficult for even large providers, can potentially limit the cost of requirements such as encryption. Segmentation alone may lead to a false sense of security. When done in combination with MFA you can require additional steps for authentication only when specific risks or conditions occur (such as access from home). An inventory of SaaS and service providers in use is critical to an implementation of MFA that matches with safeguard rules. Again, work with your IT vendor to determine whether such segmentation or other restrictions can assist your implementation efforts.

F. Disposal Procedures. You must implement procedures to securely dispose of customer information within certain specified timeframes. The Revised Rule allows you to keep consumer information as long as it is "necessary for business operations or for other legitimate business purposes," or is required to be maintained by law or regulation, or if it cannot feasibly be destroyed due the way the information is maintained.[44] If none of these factors are present, you are supposed to securely dispose of it within two years after the last time the information is used in connection with providing a product or service to the customer. However, **as a practical matter**, you need to keep certain customer information for business operations or other legitimate business purposes for a longer period of time, and you need to assess this on a case-by-case basis. You should also apply similar rules to service providers who store customer information on your behalf that you need to keep for business reasons, and also identify service providers that do not need to keep customer information in order to require them to delete the data after use. Additionally, you are required to periodically review your data retention policy to minimize the unnecessary retention of data.

At a minimum, your records disposal policy should include a requirement that personnel shred customer information prior to disposal; use secure waste bins; and use reputable document disposal vendors.

Compliance Tip

While there is little guidance on what a "legitimate business purpose" would entail, dealers may have important reasons for keeping certain records. Depending on the circumstances, a "legitimate business purpose" to keep certain records may include an ongoing relationship with the customer, contractual obligations with banks, and outside audit requirements. Additionally, dealers may have many different document retention obligations, including for legal and regulatory compliance purposes, and the Revised Rule does not override those obligations. The Revised Rule does NOT create a new blanket requirement to delete data after two years (although it clearly expresses the FTC's opinion that two years is a reasonable retention period without a legitimate business purpose). Dealers should work with legal counsel to determine the scope of their disposal policies and should consider whether to define specific business purposes for maintaining records, for ease of clarity and ease of compliance.

G. Change Management Procedures. The Revised Safeguards Rule requires businesses to implement change management procedures, which govern the addition, removal, or modification of elements of an information system. Specifically, dealerships must develop procedures to evaluate the security of devices, networks, and other items to be added to their information system, or the impact of removing such items or revising the structure of the information system.

For example, if you engage a new software vendor, or change vendors, or if you add servers or other hardware to your information system, you would need to put procedures in place to evaluate the security of the new software or new system components. This step does not require you to take any specific action with respect to such changes, but it does require you to adopt a procedure for doing so. Further, you should consider whether any of the changes will require an additional risk assessment, as described in Step Two above.

H. Monitoring and Logging of Authorized User Activity. Under the Revised Safeguards Rule, dealerships are required to implement policies and procedures that monitor the activity of authorized users and detect unauthorized access or use of customer information by such users. Your business should also log personnel activity when accessing systems containing customer information.

Again, the Revised Rule does not specify what steps must be included in these policies and procedures, just that you adopt them. This requirement is in addition to the regular testing and monitoring you must do of your information systems, as discussed in Step Four. Instead, this requirement is focused to a large extent on enabling companies to understand what information was accessed in case of a security event.

IT GUIDANCE

This is another area where taking advantage of industry available security can be beneficial. When the recommendations on MFA are followed, the area for monitoring and logging may become greatly reduced. For the less complex environments, it becomes an effort to ensure logging of activity while allowing MFA and the system to supply the monitoring. When SaaS and other systems are integrated into MFA, the overhead of monitoring and identifying "unauthorized or improper" access becomes simpler. The order of efforts should be: MFA implementation, logging of access, then threat management or behavioral analytics systems (an advanced effort). For CRM, financial, and service providers with high-risk data, the expectation should be that they have proper audit logging integrated into their application. Such efforts externally are infeasible. Internally, a combination of logging and compensating controls (such as managing access permissions) is most feasible.

STEP FOUR: Regularly Test or Audit the Effectiveness of Your Safeguards' Key Controls, Systems, and Procedures

Once you have established your information security program and its attendant controls, your job has just begun. The Rule already requires you to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. The Revised Rule specifically requires regular testing of those safeguards that are critical for detecting actual and attempted attacks on information systems. Additionally, the Revised Rule, unlike the original rule, specifies how frequently monitoring or testing of information systems should occur, and what type of testing is required. In particular, as to information systems, it requires either continuous monitoring or a combination of both penetration testing and vulnerability assessments.[45]

Specifically, as of January 10, 2022, dealerships are required to include, as part of their regular testing, a test of controls to detect actual and attempted attacks on, or intrusions into, information systems that contain customer information. This may already be a part of your information security program; the FTC appears to view this as a clarification of existing requirements.

Beginning on December 9, 2022, as we have noted, you are required to implement either continuous monitoring of your information systems or annual periodic penetration testing and vulnerability assessments.

The Revised Safeguards Rule defines "penetration testing" as a test methodology by which one attempts to circumvent or defeat security measures by trying to breach databases or controls from outside and inside your information systems. Absent continuous monitoring, you must conduct penetration testing on an annual basis. A vulnerability assessment involves systemic scans or reviews of your information systems reasonably designed to identify publicly known security vulnerabilities based on the risk assessment. Absent continuous monitoring, you must conduct vulnerability assessments at least every six months; whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

IT GUIDANCE

Continuous monitoring can be a relatively extensive requirement, requiring you to implement systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities. In our experience, we suggest that qualified individuals for non-enterprise-size dealers consider a mix of monitoring and testing. Many risks, malwares, and attacks are successful due to a lack of basic patching. This is directly related to having effective vulnerability scans. Our recommendation is a patch management solution that provides vulnerability scanning at least monthly (weekly is better). The goal is to keep systems secure and patch with a scan to prove it. This process should be kept simple. If the systems are not integrated or more advanced vulnerability scanning is used, then weekly patching for workstations and monthly for servers, followed by either a monthly or quarterly intensive vulnerability scan. Penetration tests are generally held to once per year and are human-led efforts, not automated processes. The continuous monitoring should be more part of the behavioral analytics and authentication monitoring in order to add value.

STEP FIVE: Implement Policies and Procedures for Personnel to Implement Your Information Security Program

Overall, the Revised Rule requires both security training for general personnel and utilization of qualified information security personnel, and related training and updates. The latter requirement can be fulfilled by hiring service providers to fulfill those functions.

In particular, the Revised Rule requires:

- Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment.
- Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program.
- Providing information security personnel with security updates and training sufficient to address relevant security risks.
- Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

What Employee Training Programs Must I Implement?

You must provide your personnel with security awareness training that is informed by risks identified in your periodic risk assessments and appropriate for your dealership. You may use third-party-provided programs if they meet the information security needs of your business. Additionally, updates to your employee training programs are required when there are changes in your business that impact information security, or when you identify new security threats.

Do I Need to Hire Employees Capable of Managing Information Security? If So, Do Those Individuals Need to Be Trained?

You must utilize qualified information security personnel to manage information security risks and oversee your information security program. While the Revised Safeguards Rule does not define the term "qualified," you must ensure that your information security staff have the abilities and expertise to perform the duties required in your information security program. You may accomplish this by hiring or training employees, or by hiring and training third parties to manage your business's information security. Therefore, the required staffing for this requirement will vary greatly depending on the size of your dealership and whether you use service providers to satisfy this obligation.

The Revised Safeguards Rule also requires that you train your security personnel to address new and evolving security risks. Small dealerships may consider accessing training resources online, including published security updates, online courses, and educational publications. If you use a service provider that provides assurances that personnel will be trained in current security practices, no separate training is required.

You must further verify that your information security personnel are taking steps to stay abreast of developments regarding evolving information security threats. Smaller dealerships could fulfill this requirement by, among other things, offering incentives or funds for certain personnel to take continuing education classes; including a requirement to keep informed on security research as part of their performance reviews; and conducting an annual assessment of information security personnel's knowledge of threats to their system. If you use a service provider for your security functions, you can include these requirements in your contract.

IT GUIDANCE

Security tip: Separate your basic PC and end-user support service provider from your security service provider. A good security service provider should have a co-managed security program that helps you more easily maintain oversight.

STEP SIX: Oversee Service Providers

Most dealers are not IT specialists, so they utilize service providers to store, share, maintain, and protect customer data. In many ways, service provider oversight is at the heart of the Revised Rule requirements, because service provider compliance will address the huge portion of data security issues dealers face—that is, once you adequately select, contract with, oversee, and ensure data security requirements with your vendors.

Under the 2003 Rule, you are required to oversee your service providers by (1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for protecting customer information; and (2) obligating your service providers, through contract, to implement and establish such safeguards. The Revised Rule also requires that you (3) periodically assess your service providers based on the risk they present and the continued adequacy of their safeguards. That is, you should take steps to ensure that your current service providers maintain adequate procedures to protect customer information and detect and respond to potential security breaches.

Who Qualifies as a Service Provider?

The Revised Safeguards Rule maintains the current rule's definition of "service provider" as "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services" directly to a dealership.

Does the Revised Safeguards Rule Include Any New Service Provider Oversight Obligations?

Yes. Beginning on December 9, 2022, you must monitor your service providers on an ongoing basis to verify that they are maintaining adequate safeguards to protect any customer information that they might possess. As the FTC explains, this obligation requires you to determine the risks that service providers present and evaluate whether they continue

to provide the safeguards required by your contracts. Therefore, an extensive investigation into your service providers' information systems is not required in all circumstances.

Oversight of larger service providers, for example, might include reviewing public reports of insecure practices, changes in the services that they provide, or any security failures in the services provided. However, in circumstances when a larger dealership hires a service provider to secure sensitive customer information, as a practical matter, the dealership likely will need to review security certifications, reports, or third-party audits, and it is advisable to ask the service provider to provide those documents for your review.

IT GUIDANCE

Talk to a security-focused SME and validate the risk or potentially create compensating controls so that you can keep your smaller more custom-focused vendors. Quite often the cost of putting security "around" a small vendor is much cheaper then uprooting and migrating to a new business system.

What Do I Do If My Vendor Does Not or Cannot Cooperate?

There are hundreds of technology and other vendors that serve the dealer community, ranging from start-up technology firms to more established repeat players—and as noted above, they may vary in their level of cooperation in response to your requests. You should understand that the FTC will ultimately hold you responsible if you continue to provide customer information to any particular service providers without taking the required steps to try to ensure that customer information is appropriately safeguarded by the service provider. Therefore, if your service provider cannot or will not be cooperative, in the FTC's view, you should cease doing business with the service provider.[46]

How Often Must I Review My Service Providers' Practices?

Continuous monitoring of your service providers is not required. Rather, conduct reviews of your service providers' information security practices on a periodic basis. As a practical matter, you should consider setting a periodic schedule for review of service provider practices in connection with your periodic risk assessments.

It is unclear exactly what "review" is needed to meet this requirement. What is clear, is that for the most sensitive data, the FTC has stated that certification from the service provider is not enough. Thus it would be prudent to require your service providers by contract to agree to third-party security audits, and it is arguable that in some circumstances such audits are required.

STEP SEVEN: Draft Your Incident Response Plan

This is an additional REQUIRED WRITTEN DOCUMENT that you must have by the compliance deadline.

Beginning on December 9, 2022, the Revised Safeguards Rule requires you to establish a written incident response plan that is designed to help you promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your dealership's control. Information within your dealership's control includes information stored in the cloud, but not information transmitted to a third party over which you no longer have control.

What this means is that you must plan, in advance, what actions you will take in the event of a "security event." The Revised Rule defines a "security event" broadly—an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form[47] —and it is unclear what a "security event" fully entails. The FTC has stated that it includes more than an actual data breach, and instead includes instances of "disruption or misuse" of information systems.[48] Further, it encompasses incidents even where there is no risk of consumer harm, and even where only encrypted information is compromised.[49] Indeed, the agency adopted these statements in rejecting arguments from NADA that the definition should be sensibly narrowed. As a result, even *unsuccessful* attacks could potentially meet the definition.

While the Revised Rule does not say exactly what must be in this document, it does list certain areas that must be "addressed." This written incident response plan must address the following:

- The goals of the plan.
- The internal processes for responding to a security event.
- The definition of clear roles, responsibilities, and levels of decision-making authority.
- External and internal communications and information sharing.
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.
- Documentation and reporting regarding security events and related incident response activities.
- The evaluation and revision as necessary of the incident response plan following a security event.

Again, the FTC does not state what your incident response plan must state about these issues, only that it must address each.

As a practical matter, the plan does not need to address every security event that may occur. Rather, you should focus on events that would "materially" affect customer information and should establish a system that can facilitate your dealership's response to security events, regardless of their nature. A more detailed written plan is recommended for companies with more complicated information systems or information security personnel hierarchies. The FTC provides off-the-shelf resources for businesses to design incident response plans,[50] and a sample outline of an incident response plan is included in the template information security program in Appendix A.

As with similar policies and procedures, it may not be enough to simply draft this document. You should consider practicing your incident response—either with the help of an outside IT firm or other advisor, or on your own. And of course, in the event of an incident, you must ensure you follow the plan you have adopted as closely as possible.

STEP EIGHT: Prepare an Annual Report to the Board or Equivalent

The Revised Safeguards Rule requires that your Qualified Individual make *written* reports on at least an annual basis to your board of directors. If your company does not have a board of directors, then your Qualified Individual must make this report to a senior company official responsible for overseeing your information security program. The Qualified Individual's written report should discuss the overall status of the information security program, the company's compliance with the Revised Safeguards Rule, and material matters related to the company's information security program. Such material matters should include, but are not limited to:

- Risk assessments.
- Risk management and control decisions.
- Service provider arrangements.
- The results of penetration testing.
- Security events and violations, coupled with responses to such events and violations.
- Recommended changes to information security programs.

Your board of directors or designated senior company official is not required to certify the Qualified Individual's regular reporting on the information security program.

Compliance Tip

While not expressly stated, this written reporting requirement is clearly intended to force the Qualified Individual to memorialize certain risk/benefit evaluations and other decisions made regarding the dealership's information security program. If you experience a security event or your information security practices are scrutinized, this document is likely to be closely reviewed. Additionally, under those circumstances, third parties are likely to review the reports with "20/20 hindsight" and it will be important that the bases of important decisions are well-documented. It would be prudent to ensure that this report is reviewed by your attorney.

Finally, this reporting requirement does not apply to dealerships with records on fewer than 5,000 consumers.

OVERVIEW OF APPENDIX MATERIALS

Appendix A includes a sample written information security program, including components such as an incident response plan, that is designed to be a starting point from which you can develop your own information security program and compliance procedures in alignment with the Revised Safeguards Rule. The sample is **not intended to be a turnkey product that you can simply adopt as your own.** Rather, it is a template that may be appropriate for you to draw from in preparing your own written program. As discussed in the guide, you should design a program that aligns with your specific circumstances. And because each dealership's operations are different, it is unlikely that any two information security programs will be alike. Please take care to work with your staff, vendors, and legal counsel to prepare an information security program that is right for your situation.

Appendix B includes links to IT support and guidance provided by federal government agencies, including the Cybersecurity & Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), the FTC, and others.

Sample contract terms are being developed. In the meantime, please work with your attorney to ensure that your vendor contracts comply with the requirements of the amended Safeguards Rule.

Appendix A: Sample Written Information Security Program

This Sample Written Information Security Program was prepared and provided by ComplyAuto.

As noted above, this sample document is provided as guidance only. You should not simply adopt this sample as your own. You can certainly use this as a starting point if you wish, but you must ensure that you adapt and customize your written information security program to your specific operation, systems, and based on the work of your qualified individual.

The sample below contains all of the elements required under the Revised Rule, including the information security program, incident response plan, change management and data retention procedures and policies.

Note also that Section 6.4 of the sample below includes a number of controls intended for dealers who wish to follow *additional, more extensive* requirements called the CIS Controls. While these more expansive controls are included in the sample for your reference, it is important to note that these are not required to meet the basic requirements of the Revised Rule. If you are interested in addressing these additional controls, work with your vendor and legal counsel.

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

[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 provi-

sions 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 obliga-

tion 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. 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 processors 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. 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 Record Retention Schedule contained in this policy, must be retained for the amount of time indicated in the Record 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 record 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 a Record Retention Schedule made available by their state's dealership trade association or accounting/law firm]

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 remedial 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, the District of Columbia, Puerto Rico, and the Virgin Islands 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].

Appendix B: CISA and Related Government IT Guidance Materials

CISA resources addressing software and/or cyber vulnerabilities:

Alerts and Tips: CISA National Cyber Awareness System – US-CERT

- This page contains various tips and advice about security issues for non-technical computer users.

CISA Coordinated Vulnerability Disclosure (CVD) Process

- This page discusses CISA's program to coordinate the remediation and public disclosure of newly identified cybersecurity vulnerabilities.

Defending Against Software Supply Chain Attacks

- This page discusses software supply chain risks and provides recommendations on how software customers and vendors can utilize frameworks developed by NIST to prevent software supply chain attacks.

Free Cybersecurity Services and Tools

- This page contains a compilation of free cybersecurity tools and services to help organizations further advance their security capabilities.

Known Exploited Vulnerabilities Catalog

- This page is kept up-to-date and offers subscriptions to update bulletins.

Other CISA resources:

Cyber Essentials

- This page provides a guide to understanding and implementing organizational cybersecurity practices for leaders of businesses and stakeholders.

Detection and Prevention

- This page discusses information, resources, and programs that assist critical infrastructure stakeholders in detection and prevention of cybersecurity threats.

More CISA Links:

Blog

COVID-19 Response

Cyber Resource Hub

Cybersecurity Directives

Homepage

National Strategy to Secure Cyberspace

Newsroom

Publications Library

Webinar Series - YouTube

FTC Links:

Cybersecurity for Small Business

Data Breach Response: A Guide for Business

Data Security

OnGuardOnline

Start with Security: A Guide for Business

Understanding the NIST cybersecurity framework

NIST Links:

Computer Security Resource Center

Security and Privacy Controls for Information Systems and Organizations (NIST 800-53)

Other Links:

Carnegie Mellon Software Engineering CERT Coordination Center

The SysAdmin, Audit, Network, Security (SANS) Institute: The Twenty Most Critical Internet Security Vulnerabilities

15 U.S. Code Chapter 94 - Privacy

Notes

[1] 16 C.F.R. § 314.

[2] 16 C.F.R. § 314.

[3] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272 (Dec. 9, 2021). The Rule applies to all "financial institutions," and for the reasons described here, that designation includes most, if not all, franchised dealers.

[4] There are limited exemptions, discussed below, for smaller institutions that maintain customer information for fewer than 5000 individuals.

[5] 16 C.F.R. § 313.

[6] See the NADA *Driven* Guide to the FTC Privacy Rule and the Model Privacy Notice.

[7] Note that the GLB notice and safeguarding requirements apply to information you obtain as part of insurance transactions as well, but the rules applicable to that data are issued by each state's Insurance Commissioner and are not covered in this guide. Information on this topic should be available from the agency that regulates insurance products in your state.

[8] The Revised Safeguards Rule defines nonpublic personal information as "personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." Revised 16 C.F.R. § 314.2(l)(1). "Personally identifiable financial information" is defined, in turn, as "any information a consumer provides to you to obtain a financial product or service from you; about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer." Revised 16 C.F.R. § 314.2(n)(1).

[9] Revised 16 C.F.R. § 314.2(l)(1).

[10] Your manufacturers, finance companies, banks, or your insurance carrier may also impose data security requirements on your dealership via contract. Those requirements are outside the scope of this guide but note that full compliance with the GLBA Safeguards Rule may be a contractual requirement, or it may be a useful factor when you are establishing your dealership's comprehensive data security qualifications.

[11] The Revised Safeguards Rule, as well as the FTC's latest revision to its Privacy Rule, do expand the definition of a covered "financial institution" to include what are known as "finders." As defined by the FTC, these are entities that act in "bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate." (Revised Rule 314.2(h)(2)(xiii)). This change may expand coverage of the Safeguards Rule to include other companies involved in auto-related transactions, though it will not directly affect dealers, as they are already covered under the Rule.

[12] 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k)(4)(6); 12 C.F.R. § 211.10(a)(2)-(3).

[13] 15 U.S.C. § 6809(9); Revised 16 C.F.R. § 314.2(d); Revised 16 C.F.R. § 314.2(b)(1).

[14] Revised 16 C.F.R. §§ 314.1(b), 314.2(a).

[15] Revised 16 C.F.R. §§ 314.1(a), 314.3.

[16] Revised 16 C.F.R. § 314.2(d).

[17] Revised 16 C.F.R. § 314.2(c). The Revised Safeguards Rule defines "consumer" as "an individual who obtains

or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative." Revised 16 C.F.R. § 314.2(b)(1). Technically, a customer relationship requires a "continuing relationship" with the consumer, but under the Rule, information you collect in the course of arranging financing is still covered, whether or not you have a literal ongoing relationship with the consumer. Revised Rule § 314.2(e)(1), (2).

[18] Revised 16 C.F.R. §§ 314.2(d), 314.1(b).

[19] 16 C.F.R. §§ 313.3(n)(1)(ii), Revised § 314.2(d).

[20] Revised 16 C.F.R. §§ 314.2(d), (l), (n).

[21] See The FTC's Financial Institutions and Customer Information: Complying with the Safeguards Rule.

[22] In addition, because your privacy notices, in all likelihood, use the model safeguards language *("we maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information")*, you could be subject to an enforcement action or a UDAP claim for violating the Privacy Rule as well, to the extent this was not an accurate statement. See NADA's Dealer Guide to the FTC Privacy Rule and the Model Privacy Notice.

[23] 16 C.F.R. 314.4(a).

[24] Indeed, the revised rule as originally proposed by the FTC included a reference to this individual as a Chief Information Security Officer (CISO). In response to comments by NADA and others, the FTC expressly stated that this individual does NOT need to be a CISO. 86 Fed. Reg. at 70281.

[25] 86 Fed. Reg. at 70281-82.

[26] 86 Fed. Reg. at 70280.

[27] Note that dealers that maintain information on fewer than 5,000 customers are exempt from the requirements of a written assessment containing these elements but **must still conduct** periodic risk assessments and base information security programs on them. Revised 16 C.F.R. § 314.6.

[28] As outlined below, your risk assessment may guide you in exactly how you implement these steps in practice, but to be clear, you have to take these steps in any event.

[29] An "authorized user" is defined as "any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data." Revised Rule 314.2(a). It therefore includes employees as well as outside parties and others. As noted in the text, you will need to establish different access rules for different kinds of users, based on the kind of data they need to access.

[30] It remains an open question as to how extensively you should inquire as to downstream sharing of customer information by companies receiving that data from service providers (and companies further downstream). However, given that the Rule requires evaluation and addressing of risk related to the security, confidentiality, and integrity of customer information, you should consider implementing procedures to fully understand downstream sharing so you can mitigate risks appropriately.

[31] 86 Fed. Reg. at 70296.

[32] The FTC notes, for example, in the context of the encryption requirement: "A financial institution that uses a service provider to store and process customer information must require that service provider to encrypt that information and periodically determine whether it continues to do so. If it is infeasible for the service provider to meet these requirements, then the financial institution's Qualified Individual must work with the service provider to develop compensating controls or cease doing business with the service provider." *Id.* at 70288 n. 172.

[33] Revised 16 C.F.R. § 314.2(f).

[34] Most state data breach laws also refer to encrypted data, and many of them define that term. However, the FTC rejected alternative formulations of the definition that would more closely align with many of those state laws. Therefore, if you have implemented encryption in reliance on state law definitions, you should consult with IT professionals and counsel to determine whether additional steps are needed to comply with the Revised Safeguards Rule, and not assume your current encryption standards are sufficient.

[35] 86 Fed. Reg. at 70275.

[36] Revised 16 C.F.R. § 314.4(c)(3).

[37] 86 Fed. Reg. at 70289.

[38] *Id.*

[39] *Id.*

[40] See FTC warns companies to remediate Log4j security vulnerability. See also Apache Log4j Vulnerability Guidance for more information of this specific vulnerability.

[41] Top Free Vulnerability Scanner Software (last accessed Dec. 10, 2021).

[42] Revised 16 C.F.R. § 314.2(k). Several states substantially restrict the collection and use of biometric information, and in Illinois, for example, failure to follow biometric privacy laws can result in costly private litigation. Dealers should consult with legal counsel prior to collecting or using biometric characteristics such as fingerprints or facial scans.

[43] The FTC has expressed some disfavor with using SMS text messages as the second means of verification, based on security concerns. Ultimately, SMS text messages are allowed, but dealers must evaluate the risks of using SMS messages. The FTC has concluded that "in some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy use, if its risks do not outweigh those benefits under the circumstances. In other instances, however, the use of SMS text messages may not be a reasonable solution, such as when extremely sensitive information can be obtained through the access method being controlled, or when a more secure method can be used for a comparable price." 86 Fed. Reg. at 70277.

[44] Revised 16 C.F.R. § 314(c)(6)(i).

[45] Dealers that maintain information on fewer than 5,000 customers are exempt from this specific monitoring and penetration testing/vulnerability assessment requirement.

[46] 86 Fed. Reg. at 70288 n. 172.

[47] Revised 16 C.F.R. § 314.2(p).

[48] 86 Fed. Reg. at 70274-75.

[49] *Id.* at 70275.

[50] See Data Breach Response: A Guide for Business.

Acknowledgments

This guide was prepared for NADA by:

Duane C. Pozza, Primary Author
Partner, Wiley Rein LLP
1776 K Street NW
Washington, DC 20006
202.719.4533
dpozza@wiley.law
wiley.law

wiley

Appendix A was provided by ComplyAuto.
Chris Cleveland
Co-Founder and CEO, ComplyAuto, LLC
5900 Sycamore Canyon Blvd.
Riverside, CA 92507
385.277.5882
chris@complyauto.com
ComplyAuto.com

COMPLYAUTO PRIVACY

Professional IT guidance was provided by RedZone Technologies, LLC.
James Crifasi
COO and CTO, RedZone Technologies, LLC
1750 Forest Drive, Suite 100
Annapolis, MD 21401
410.897.9494
jcrifasi@redzonetech.net
RedZone Technologies

RedZone Technologies
410-897-9494 www.redzonetech.net

nada.org